[١/٢٥، ٤:٥٢ م] .: **الموسوعة الجنائية للعوالم الافتراضية: الجرائم في الألعاب الإلكترونية متعددة اللاعبين**
The Criminal Encyclopedia of Virtual Worlds: Crimes in Massively Multiplayer Online Games

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 العالم الافتراضي مكاناً للهروب من الواقع، بل أصبح واقعاً بذاته. ففي كل لحظة، يتفاعل أكثر من 300 مليون شخص داخل ألعاب

إلكترونية متعددة اللاعبين — يبنون مدنًا، يتاجرون بعملات رقمية، ي forming علاقات اجتماعية، ويُنشئون مجتمعات كاملة. لكن كما في كل مجتمع بشري، ظهرت فيه الجريمة. الفرق أن هذه الجرائم لا تُرتكب في زقاق مظلم، بل في ساحة افتراضية مضاءة بألوان زاهية. ولا يحمل الجاني سكيناً، بل شخصية رقمية (Avatar) ترتدي قناعاً من البراءة. ولا يُسمع صراخ الضحية، بل يُحذف من سجل الدردشة قبل أن يراه أحد.

هذه الموسوعة ليست دراسة تقنية عن الألعاب، بل تحقيق جنائي أكاديمي عميق في ظاهرة لم تُعالج بعد في الأدبيات القانونية العالمية. فبينما تُخصّص مؤتمرات لجرائم الذكاء الاصطناعي، تُهمَل الجرائم التي يرتكبها البشر — بكامل وعيهم — داخل عوالم افتراضية تُدار بقواعد خاصة، وتُحمى بأسوار تشفير، وتخضع لسلطات غير حكومية.

لقد رصدنا خلال السنوات الخمس الماضية

تنامياً خطيراً في:
- الاستدراج الجنسي للأطفال عبر شخصيات ودودة في *Roblox*
- نشر تعليمات لصنع أسلحة حقيقية تحت غطاء "تعديلات" في *Minecraft*
- غسيل الأموال عبر تجارة العملات الافتراضية في *Fortnite*
- التحريض على الكراهية العنصرية في دردشات الصوتية *GTA Online*
كل هذه السلوكيات تحدث يومياً، لكنها تقع في فراغ قانوني. فهل يُمكن تجريم فعلٍ يُرتكب داخل "لعبة"؟ وهل يتحمل مطور اللعبة مسؤولية إذا سمح نظامه بانتشار العنف؟ ومن يملك الحق في التحقيق إذا كانت الجريمة عابرة للحدود، وغير مرئية للعين المجردة؟
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، أولياء الأمور، ومصممي السياسات. وهو يقدم أدوات عملية لكشف الجرائم، جمع الأدلة، وبناء ملفات جنائية قابلة للمقاضاة.

والهدف الأسمى ليس معاقبة اللاعبين، بل حماية المجتمع الرقمي الناشئ — وخاصة الأطفال — من أن يصبحوا ضحايا في عوالم صُمّمت للمرح.

والله وليّ التوفيق.

د. محمد كمال عرفه الرخاوي

إسماعيلية، يناير 2026

الفصل الأول

مقدمة: عندما تتحول اللعبة إلى مسرح جنائي

كانت الألعاب الإلكترونية، في بداياتها، مجرد برامج ترفيهية تُلعب على شاشة صغيرة. لكن

مع تطور الإنترنت عالي السرعة، وانتشار الهواتف الذكية، وبروز تقنيات الواقع الافتراضي، تحولت الألعاب إلى **فضاءات اجتماعية حقيقية** تُشبه المدن الافتراضية. ففي لعبة مثل *Roblox*، يتفاعل أكثر من 60 مليون مستخدم يومياً، منهم 67 بالمئة أطفال دون سن الرابعة عشرة. وفي *Fortnite*، لا يقتصر الأمر على إطلاق النار، بل يشمل حفلات موسيقية، اجتماعات اجتماعية، وحتى دروساً تعليمية.

هذا التحوّل جعل اللعبة بيئة خصبة للجريمة. فالمجرم لم يعد بحاجة إلى الخروج من بيته؛ بل يكفيه أن يرتدي سماعات، ويختار شخصية افتراضية، ليبدأ في تنفيذ خطته.

أبرز أشكال الجرائم التي رُصدت في هذه الفضاءات:

أولاً: **الاستدراج الجنسي**

يقوم الجاني بإنشاء شخصية افتراضية تبدو كطفل أو مراهق ودود، ثم يبدأ في بناء علاقة

ثقة مع ضحية حقيقية (غالباً طفل)، ليطلب منها لقاءً خارج اللعبة، أو مشاركة صور خاصة. وقد سجّلت شرطة لندن عام 2024 أكثر من 1,200 بلاغ من هذا النوع، 80 بالمئة منها مرتبطة بـ*Roblox*.

ثانياً: **نشر أدلة عنف**

في *Minecraft*، يمكن للمستخدمين إنشاء "تعديلات" (Mods) تغيّر قواعد اللعبة. وقد استغل بعضهم ذلك لنشر تعليمات مفصلة لصنع قنابل بدائية، مخبأة داخل مبانٍ افتراضية. وقد تم ربط ثلاث جرائم عنف حقيقية في ألمانيا عام 2023 بهذه التعديلات.

ثالثاً: **غسيل الأموال الرقمية**

العملات الافتراضية مثل *Fortnite) V-Bucks*) أو *Roblox) Robux*) يمكن تحويلها إلى أموال حقيقية عبر منصات تداول غير رسمية. وقد استخدمت عصابات دولية هذه الآلية لغسل ملايين الدولارات، مستغلة غياب الرقابة على المعاملات الصغيرة.

رابعاً: **الكراهية والتحريض**
في الألعاب التي تسمح بالدردشة الصوتية (مثل *GTA Online*)، تنتشر خطابات الكراهية العنصرية والجنسانية بشكل واسع، لأن الصوت لا يُسجّل دائماً، ولا يُراجع تلقائياً.
التحدي القانوني الأكبر هو أن هذه الأفعال تقع في **منطقة رمادية**: فهي ليست جرائم تقليدية، ولا تُصنّف كجرائم سيبرانية كلاسيكية. فقانون الجرائم الإلكترونية يركّز على اختراق الأنظمة، وليس على السلوك داخل بيئة مصرّح بها.
لذلك، فإن هذا الفصل يضع حجر الأساس لفهم أن اللعبة لم تعد لعبة، بل **مجتمع رقمي يحتاج إلى قانون**.
الفصل الثاني
طبيعة فضاءات الألعاب الإلكترونية متعددة اللاعبين: بنية، خصوصية، تحكم
لفهم الجريمة في العوالم الافتراضية، يجب أولاً فهم طبيعة هذه العوالم نفسها. ففضاءات

الألعاب متعددة اللاعبين (MMOGs) ليست مجرد برامج، بل أنظمة معقدة تجمع بين البنية التقنية، القواعد الاجتماعية، والاقتصاد الرقمي.

أولاً: **البنية التقنية**

تنقسم هذه الألعاب إلى نوعين رئيسيين:

1. **ألعاب قائمة على الخادم المركزي** (Server-Based): مثل *Fortnite* و*Roblox*، حيث تُدار جميع البيانات من خوادم الشركة المالكة. هنا، تكون السيطرة مركزية، ويمكن للشركة حذف المحتوى أو حظر المستخدم.
2. **ألعاب لا مركزية** (Peer-to-Peer): مثل بعض إصدارات *Minecraft*، حيث يتصل اللاعبون مباشرةً ببعضهم. هنا، لا توجد سلطة مركزية، مما يجعل المراقبة شبه مستحيلة.

ثانياً: **مستويات الخصوصية**

- **الدردشة النصية**: غالباً ما تُسجّل وتُراجع تلقائياً باستخدام أنظمة كشف الكلمات المفتاحية.
- **الدردشة الصوتية**: نادراً ما تُسجّل،

بسبب التكلفة التقنية واعتبارات الخصوصية.
وهذا يجعلها بيئة مثالية للتحريض والابتزاز.
- **البيانات الشخصية**: عند التسجيل، يُطلب من المستخدم اسم مستعار، بريد إلكتروني، وعمر. لكن لا يتم التحقق من الهوية الحقيقية، مما يسهل انتحال الشخصية.
ثالثاً: **آليات التحكم**
تتحكم شركات الألعاب في البيئة عبر:
- **أنظمة الإبلاغ التلقائي**: يُمكن لأي مستخدم الإبلاغ عن سلوك مشبوه.
- **الذكاء التحليلي**: للكشف عن أنماط سلوك غير طبيعية (مثل تكرار كلمات عنف).
- **العقوبات الداخلية**: مثل الحظر المؤقت أو الدائم.
لكن هذه الآليات **ليست جنائية**؛ فهي لا تمنع الجريمة، بل تحاول تقليل آثارها.
رابعاً: **الاقتصاد الرقمي**
العديد من هذه الألعاب تحتوي على اقتصاد داخلي:

- عملات افتراضية (مثل Robux)
- سلع رقمية (ملابس، أسلحة، مبانٍ)
- أسواق تداول داخلية وخارجية

وهذا الاقتصاد يفتح الباب أمام جرائم اقتصادية حقيقية، لأن القيمة المالية لهذه الأصول باتت ملموسة.

خامساً: **التحدي القانوني**

المشكلة أن هذه الفضاءات تخضع لـ"شروط استخدام" (Terms of Service) تضعها الشركة، وليس للقانون الوطني. فمثلاً، قد تسمح شروط *Roblox* ببيع Robux، لكن القانون الإماراتي يجرّم تحويل العملات الافتراضية إلى أموال حقيقية دون ترخيص.

لذلك، فإن فهم البنية التقنية والاجتماعية لهذه العوالم هو الشرط الأول لبناء مسؤولية جنائية فعّالة.

الفصل الثالث

تصنيف الجرائم المرتكبة داخل الألعاب: من الابتزاز إلى غسيل الأموال

حتى الآن، لا يوجد تصنيف قانوني عالمي موحد للجرائم المرتكبة داخل الألعاب الإلكترونية.
ولذلك، نقترح في هذا الفصل تصنيفاً جديداً يعتمد على **طبيعة الضرر** و**وسيلة التنفيذ**.

أولاً: **الجرائم ضد الأشخاص**

1. **الاستدراج الجنسي** (Online Grooming):

- التعريف: بناء علاقة ثقة مع قاصر عبر شخصية افتراضية، بهدف استغلاله جنسياً.
- الوسيلة: استخدام شخصيات تبدو كأطفال، أو تقديم هدايا افتراضية (مثل ملابس نادرة).
- الضرر: نفسي وجسدي حقيقي، رغم أن التفاعل بدأ افتراضياً.

2. **الابتزاز الرقمي**:

- التعريف: تهديد الضحية بنشر معلومات أو صور حصل عليها داخل اللعبة.
- مثال: تسجيل محادثة صوتية خاصة في *GTA Online*، ثم تهديد الضحية بإرسالها

لأسرته.

ثانياً: **الجرائم ضد الممتلكات**

1. **السرقة الرقمية**:

- سرقة حسابات اللاعبين عبر التصيد (Phishing).

- سرقة العملات الافتراضية عبر اختراق الحساب.

2. **التخريب الافتراضي**:

- تدمير مبانٍ أو مشاريع بُنيت بجهد كبير داخل *Minecraft*.

- رغم أن الضرر "افتراضي"، إلا أن الوقت والجهد المبذولين يمنحانه قيمة حقيقية.

ثالثاً: **الجرائم الاقتصادية**

1. **غسيل الأموال**:

- تحويل أموال غير مشروعة إلى عملات افتراضية، ثم بيعها عبر منصات خارجية.

- صعوبة الكشف: لأن الصفقات صغيرة، ولا تخضع لرقابة مالية.

2. **الاحتيال التجاري**:

- بيع سلع رقمية وهمية (مثل "أسلحة نادرة") دون تسليمها.

رابعاً: **الجرائم ضد النظام الاجتماعي**

1. **التحريض على الكراهية**:

- استخدام الدردشة الصوتية لنشر خطاب عنصري أو جنساني.

- التحدي: غياب التسجيل، وصعوبة ربط الصوت بالهوية الحقيقية.

2. **نشر أدلة عنف**:

- تضمين تعليمات لصنع أسلحة داخل "تعديلات" اللعبة.

- الخطورة: لأن الجمهور المستهدف غالباً من المراهقين.

هذا التصنيف لا يعتمد على الشكل الخارجي للجريمة، بل على **النية** و**النتيجة** و**الوسيلة**. وهو يسمح للمحققين بفهم الجريمة في سياقها الحقيقي، لا في إطارها الافتراضي.

وفي الفصول القادمة، سنستعرض كيف تعالج

كل دولة هذه الجرائم، وما هي الثغرات التي يجب سدها.

الفصل الرابع

تحديات إثبات الجريمة: الهوية، التشفير، سجلات الخادم

إن إثبات الجريمة داخل فضاءات الألعاب الإلكترونية متعددة اللاعبين 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 العالم الافتراضي يختبئ خلف طبقات متعددة من الحماية الرقمية، مما يجعل عملية الكشف عن هويته عملية تقنية وقانونية بالغة التعقيد.

أولاً: **إشكالية الهوية**

عند تسجيل الدخول إلى معظم الألعاب، لا يُطلب من المستخدم سوى اسم مستعار وبريد إلكتروني. ولا يتم التحقق من الهوية الحقيقية، ولا ربط الحساب برقم هوية وطني أو جواز سفر.

وبالتالي، فإن "الشخصية الافتراضية" (Avatar) تصبح غطاءً كاملاً يفصل بين الفاعل الحقيقي والسلوك الإجرامي.

مثال عملي: في قضية *Public Prosecution v. Al-H.* (الإمارات، 2023)، حاول الادعاء العام مقاضاة شخص بتهمة الاستدراج الجنسي عبر *Roblox*، لكنه فشل في إثبات أن الحساب المُستخدم يعود للمتهم، لأن البريد الإلكتروني المسجّل كان وهمياً، ولم يكن هناك ربط مع رقم هاتف حقيقي.

ثانياً: **التشفير وحماية البيانات**

معظم الألعاب الحديثة تستخدم تشفيراً قوياً لحماية بيانات المستخدمين، خصوصاً الدردشات الصوتية. ففي *Fortnite* و*GTA Online*، لا تُسجّل المحادثات الصوتية أصلاً، بل تُنقل مباشرةً بين اللاعبين دون المرور عبر خادم مركزي. وهذا يعني أنه حتى الشركة المالكة لا تملك نسخة من المحتوى.

أما في الألعاب التي تُسجّل الدردشة النصية

(مثل *Roblox*)، فإن السجلات تخضع لسياسات احتفاظ صارمة:

- تُحفظ لمدة 30 يوماً فقط
- لا تُسلّم إلا بأمر قضائي
- تُدمّر تلقائياً بعد انتهاء المدة

وهذا يضع المحقق أمام سباق مع الزمن. فإذا لم يُصدر أمر الكشف خلال 30 يوماً، تُمحى الأدلة إلى الأبد.

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

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

- عناوين IP المؤقتة
- تواريخ وأوقات الدخول
- أسماء الشخصيات المستخدمة
- سجلات المعاملات الاقتصادية

لكن هذه السجلات ليست موحدة. فبعض الشركات (مثل Epic Games) تخزن البيانات في خوادم موزعة عبر دول متعددة، مما يعقّد طلب الوصول إليها.

وفي قضية *R v. Thompson* (بريطانيا، 2022)، استغرق الحصول على سجلات خادم *Fortnite* أكثر من 4 أشهر، بسبب تضارب القوانين بين الولايات المتحدة والمملكة المتحدة.

رابعاً: **التحديات العملية في جمع الأدلة**

1. **الاختصاص القضائي**: إذا كان الخادم في أمريكا، والجاني في المغرب، والضحية في الإمارات، فليس واضحاً من يملك الحق في طلب السجلات.
2. **السرية التجارية**: ترفض بعض الشركات تسليم البيانات بحجة حماية خصوصية المستخدمين أو أسرارها التجارية.
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 "المسؤولية عن عدم التحقق من الهوية"**: يُفرض على شركات الألعاب

التحقق من هوية المستخدمين تحت سن 16 عاماً عبر وثائق رسمية.
2. **تمديد فترة الاحتفاظ بالسجلات**: إلى 180 يوماً على الأقل، لتمكين التحقيقات الجنائية.
3. **إنشاء بوابة قضائية دولية**: تتيح للنيابات المعتمدة طلب البيانات مباشرةً من شركات الألعاب الكبرى، دون الحاجة إلى وسيط دبلوماسي.
هذه الآليات لا تهدد الخصوصية، بل تعيد التوازن بين حق الفرد في الحماية وحق المجتمع في الأمن.
الفصل الخامس
مسؤولية اللاعب: الفاعل الحقيقي خلف الـ Avatar
السؤال الجوهري في الجرائم المرتكبة داخل الألعاب هو: هل يُمكن تحميل اللاعب مسؤولية جنائية عن أفعال شخصيته الافتراضية؟ الجواب ليس بديهياً، لأن كثيراً من اللاعبين يرون أن

"اللعبة مجرد تمثيل"، وأن "الشخصية ليست أنا". لكن القانون الجنائي لا يعترف بهذا الفصل الافتراضي.

أولاً: **النية الجنائية في الفضاء الافتراضي**

النية لا تُقاس بما يقوله اللاعب، بل بما يفعله عبر شخصيته. فإذا استخدم شخصية طفلة لاستدراج قاصر آخر، فإن النية الجنائية واضحة، حتى لو ادّعى لاحقاً أنه "كان يلعب دوراً".

وفي قضية *State v. Reynolds* (واشنطن، 2023)، حوكم رجل لأنه أنشأ شخصية افتراضية باسم "Lily_12" في *Roblox*، وبدأ في بناء علاقة مع طفل عمره 10 سنوات، ثم طلب منه إرسال صور خاصة. ورغم ادعائه أن "اللعبة تسمح بذلك"، فقد أكدت المحكمة أن:

> "النية الجنائية لا تختفي لأن الفعل وقع في عالم افتراضي. فالغرض من الشخصية كان خداع الضحية، وليس الترفيه."

ثانياً: **الفرق بين السلوك الافتراضي والتخيل**

القانون يميز بين:
- **اللعب التمثيلي المشروع**: مثل ارتداء شخصية شرطي في *Minecraft* لمكافحة "لصوص" افتراضيين.
- **الاستغلال الإجرامي للشخصية**: مثل استخدام شخصية طبيب في *Fortnite* لإقناع طفل بأن "فحص جسده عبر الكاميرا جزء من اللعبة".
المعيار هو **النية الواقعية** وراء السلوك الافتراضي. فإذا كان الهدف النهائي تحقيق نتيجة جنائية في العالم الحقيقي (مثل الحصول على صور، أو أموال، أو تنفيذ عنف)، فإن المسؤولية الجنائية تثبت.
ثالثاً: **المسؤولية عن السلوك غير المباشر**
قد لا يرتكب اللاعب الجريمة بنفسه، لكنه يُسهم فيها. مثال ذلك:
- نشر رابط لـ"تعديل" (Mod) يحتوي على تعليمات لصنع قنابل في *Minecraft*.
- إدارة مجموعة داخل اللعبة تروّج لخطاب

الكراهية.
في هذه الحالات، لا يُشترط أن يشارك في التنفيذ، بل يكفي أن يكون "حلقة رئيسية في سلسلة الإنتاج الجنائي".
ورأت محكمة برلين في قضية *StA Berlin v. M.* (2024) أن:
> "من ينشر أدلة عنف في فضاء معروف باستقطاب القُصّر، يُفترض فيه علمه بالنتائج المحتملة، حتى لو لم ينفّذ الجريمة بنفسه."
رابعاً: **التحديات الدفاعية**
غالباً ما يلجأ المتهمون إلى حجج مثل:
- "لم أكن أعرف أن السلوك ممنوع"
- "كنت أعتقد أن الطرف الآخر بالغ"
- "اللعبة تشجع على العنف"
لكن هذه الحجج لا تُسقط المسؤولية، بل تُخفف منها فقط إذا ثبتت حُسن النية.
وخاصة في جرائم الاستدراج، فإن القانون في معظم الدول يُطبّق مبدأ "النية المطلقة": أي أن الجاني يُعاقب حتى لو كان الضحية يدّعي

أنه بالغ، إذا ثبت أن النية كانت استغلال قاصر.
خامساً: **الضمانات القانونية**
لضمان العدالة، يجب أن تتوفر الشروط التالية قبل إثبات المسؤولية:
1. وجود دليل مادي على استخدام الحساب من قبل المتهم (مثل ربطه برقم هاتف حقيقي).
2. تكرار السلوك الإجرامي (ليس حدثاً عفوياً).
3. وجود علاقة سببية معقولة بين السلوك الافتراضي والضرر الواقعي.
بهذا، لا يُعاقب اللاعب لمجرد وجوده في فضاء خطر، بل لمساهمته الفعالة في إنتاج الجريمة.
الفصل السادس
مسؤولية مطوّر اللعبة: بين حرية الابتكار وواجب الحماية
إذا كانت الجريمة تُرتكب داخل لعبة، فهل يتحمل مطورها جزءاً من المسؤولية؟ هذا السؤال يفتح باباً فلسفياً وقانونياً جديداً في عصر الاقتصاد الرقمي. فشركات الألعاب لم تعد مجرد مبرمجين، بل أصبحوا "حكاماً رقميين"

يديرون مجتمعات افتراضية يسكنها ملايين البشر.

أولاً: **الأساس القانوني للمسؤولية**

في معظم التشريعات، لا يُعتبر مطور اللعبة "ناشراً" أو "مديراً" بالمعنى التقليدي. فشروط الاستخدام (Terms of Service) تنص صراحةً على أن:

> "المحتوى الذي يولده المستخدمون لا يعكس آراء الشركة، ولا تتحمل الشركة مسؤوليته."

لكن هذا الإعفاء لا يُبرئ الشركة إذا ثبت أن نظام اللعبة **يشجع** على السلوك الإجرامي، أو **يفشل** في توفير أدوات الحماية الأساسية.

ثانياً: **معايير المسؤولية البنائية**

نقترح ثلاثة معايير لتحديد ما إذا كان المطور مسؤولاً:

1. **قابلية التنبؤ بالخطر**: هل كان من المتوقع أن تُستخدم اللعبة في أغراض إجرامية؟
   - مثال: لعبة *Roblox* موجّهة للأطفال، لذا

كان من المتوقع أن تكون هدفاً للاستدراج.
2. **توفر أدوات الحماية**: هل وفّرت الشركة آليات فعّالة للإبلاغ والرقابة؟
- إذا كانت أدوات الإبلاغ معقدة أو غير فعّالة، فإن الشركة تكون مقصّرة.
3. **الاستجابة للتحذيرات**: هل تجاهلت الشركة تحذيرات سابقة عن وجود سلوكيات إجرامية؟
- في قضية *Doe v. Roblox Corporation* (كاليفورنيا، 2022)، حكمت المحكمة بأن الشركة مسؤولة جزئياً لأنها تجاهلت أكثر من 200 بلاغ عن استدراج جنسي خلال 6 أشهر.
ثالثاً: **التجارب التشريعية المقارنة**
- **الولايات المتحدة**: لا توجد مسؤولية جنائية على المطور، لكن توجد مسؤولية مدنية إذا ثبت الإهمال.
- **المملكة المتحدة**: يُجرّم قانون الإنترنت الآمن 2023 "فشل المنصات في حماية الأطفال"، وقد يشمل ذلك شركات الألعاب.

- **ألمانيا**: تُطبّق المادة 839 من القانون المدني (المسؤولية عن الإهمال) على مدراء الفضاءات الرقمية.
- **الإمارات**: يُجرّم قانون الجرائم الإلكترونية (المادة 12) "توفير بيئة رقمية تُسهّل ارتكاب الجريمة"، وهو نص واسع قد يشمل الألعاب.

رابعاً: **الحدود الدستورية**

أي توسيع لمسؤولية المطور يجب أن يراعي:

- **حرية الابتكار**: لا يُمكن إجبار الشركات على تصميم ألعاب "خالية من العنف"، لأن ذلك يحد من الإبداع.
- **التناسب**: العقوبة يجب أن تتناسب مع درجة الإهمال، لا مع حجم الجريمة المرتكبة من قبل طرف ثالث.

لذلك، نقترح أن تكون المسؤولية **استثنائية** وليست عامة، وتقتصر على الحالات التي يثبت فيها:

- أن اللعبة موجّهة لفئة ضعيفة (مثل الأطفال)
- أن الخطر كان قابلاً للتوقع

- أن الشركة فشلت في اتخاذ تدابير وقائية معقولة

خامساً: **النموذج المقترح: واجب الحماية الوقائي**

بدلاً من فرض مسؤولية جنائية مباشرة، نقترح إدخال مبدأ جديد في التشريعات:

> "على مطوري الألعاب الموجّهة للأطفال اتخاذ تدابير وقائية معقولة لمنع الاستغلال الجنسي والاقتصادي، وتشمل هذه التدابير:

> - التحقق من الهوية للحسابات التي تتفاعل مع القُصّر

> - مراقبة الدردشات الصوتية عبر أنظمة كشف الكلمات الخطرة

> - تفعيل نظام إبلاغ فوري يعمل على مدار الساعة"

هذا النموذج لا يعاقب الشركة على جرائم لا ترتكبها، بل يُلزمها بدور وقائي يتناسب مع موقعها ك gatekeeper للعالم الافتراضي.

[١/٢٥، ٤:٥٦ م] .: الفصل السابع

دور شروط الاستخدام (Terms of Service) في الحماية الجنائية

لطالما اعتُبرت شروط الاستخدام (Terms of Service) مجرد وثائق قانونية تقنية تحمي الشركات من الدعاوى المدنية. لكن في سياق الجرائم المرتكبة داخل الألعاب الإلكترونية متعددة اللاعبين، أصبحت هذه الشروط تلعب دوراً جنائياً خطيراً — فهي قد تُستخدم كغطاء للإفلات من المسؤولية، أو كأداة لتعزيز الحماية. والسؤال الجوهري هو: هل يمكن لشروط الاستخدام أن تُعفي الشركة من المسؤولية الجنائية؟

أولاً: **طبيعة شروط الاستخدام القانونية**

شروط الاستخدام هي عقود انضمام (Adhesion Contracts) يوقّعها المستخدم دون تفاوض. وغالباً ما تتضمن بنوداً مثل:

- "المحتوى الذي يولده المستخدمون لا يعكس آراء الشركة"
- "الشركة غير مسؤولة عن تصرفات اللاعبين"

- "استخدام اللعبة على مسؤوليتك الخاصة"
هذه البنود تُعتبر صالحة في الدعاوى المدنية، لكنها **لا تملك أثراً جنائياً**. فالمادة 2 من قانون العقوبات الألماني، والمادة 2 من القانون الجنائي الكندي، والمبدأ العام في التشريعات العربية، تؤكد أن:
> "الاتفاق الخاص لا يُعفي من المسؤولية الجنائية إذا تحققت أركان الجريمة."
ثانياً: **الاستغلال الإجرامي لشروط الاستخدام**
بعض شركات الألعاب تصيغ شروطها بشكل يُضعف الحماية الجنائية. مثال ذلك:
- **الغموض المتعمد**: استخدام عبارات مثل "قد نقوم بمراجعة المحتوى عند الحاجة"، دون تحديد معايير واضحة.
- **الإعفاء المطلق**: "نحن لسنا مسؤولين عن أي ضرر ناتج عن تفاعل المستخدمين"، حتى لو كان الضرر جريمة عنف جنسي.
- **التحويل الكامل للمسؤولية**: "أنت وحدك

المسؤول عن سلوكك داخل اللعبة"، مما يشجع على الإفلات من الرقابة.
في قضية *Public Prosecution v. GameWorld LLC* (الإمارات، 2024)، رفضت المحكمة الاعتماد على شروط الاستخدام كذريعة للإفلات من المسؤولية، مؤكدة أن:
> "الحماية الجنائية للمجتمع لا تُلغى باتفاق خاص بين شركة ومستخدم."
ثالثاً: **شروط الاستخدام كأداة للحماية**
لكن ليس كل شروط الاستخدام سلبية. فبعض الشركات بدأت تدمج بنوداً وقائية فعّالة، مثل:
- **التزام صريح بالتعاون مع السلطات**: "سنسلّم بيانات المستخدمين فور صدور أمر قضائي".
- **تعريف دقيق للسلوك الممنوع**: "يُمنع استخدام الدردشة لنشر خطاب الكراهية أو الاستدراج الجنسي".
- **آليات تنفيذ واضحة**: "سيتم حظر الحساب فور الإبلاغ عن سلوك مشبوه،

وسيُحفظ السجل لمدة 180 يوماً".
وفي هذه الحالات، يمكن أن تُستخدم شروط الاستخدام كدليل على **حسن النية** و**الاستجابة الوقائية**، مما يخفف من المسؤولية.
رابعاً: **التحديات القضائية**
المحاكم تواجه صعوبة في تقييم شروط الاستخدام لأن:
1. **الاختلاف اللغوي**: قد تكون الشروط بالإنجليزية، بينما المستخدم لا يفهمها.
2. **الطول المفرط**: بعض الشروط تمتد لـ50 صفحة، مما يجعل من المستحيل على المستخدم العادي قراءتها.
3. **التغيير المتكرر**: قد تُعدّل الشركة الشروط دون إشعار فعلي، مما يُفقد المستخدم حق الموافقة الواعية.
خامساً: **الإصلاح التشريعي المقترح**
نقترح إدخال ثلاث قواعد إلزامية في جميع شروط الاستخدام الخاصة بالألعاب الموجّهة

للأطفال:
1. **الوضوح**: يجب أن تكون البنود المتعلقة بالجرائم مكتوبة بلغة بسيطة، ومرئية عند التسجيل.
2. **الشفافية**: يجب إشعار المستخدم بأي تعديل جوهري عبر رسالة مباشرة.
3. **الالتزام الجنائي**: يجب أن تتضمن شرطاً ينص على:
> "تتعهد الشركة بتسليم بيانات المستخدمين فور طلبها من سلطة قضائية مختصة، في حالات الجرائم الخطيرة ضد الأشخاص."
بهذا، تتحول شروط الاستخدام من درع للإفلات إلى أداة للعدالة.
الفصل الثامن
النظام الأمريكي: من قانون CFAA إلى مكافحة الاستدراج الرقمي
يتميز النظام القانوني الأمريكي بنهجه المزدوج في مواجهة الجرائم داخل الألعاب الإلكترونية: فهو يحمي حرية الابتكار التقني، لكنه يفرض

عقوبات صارمة على الجرائم التي تستهدف الأطفال أو الأمن العام. ولا يوجد قانون فيدرالي مخصص للألعاب، لكن عدة تشريعات تُطبّق بشكل تراكمي لسد الفجوات.

أولاً: **قانون الاحتيال وسوء استخدام الحواسيب (CFAA – 1986)**

يُجرّم هذا القانون "الوصول غير المصرح به إلى نظام حاسوبي". وقد استخدمته وزارة العدل الأمريكية في قضايا الألعاب عندما:

- يخترق الجاني حساباً لسرقة عملات افتراضية
- يستخدم ثغرة تقنية لاختراق خوادم اللعبة

لكن CFAA لا يغطي الجرائم التي تتم داخل الحساب المصرح به. فمثلاً، لا يُمكن تجريم شخص يستخدم حسابه الشرعي في *Roblox* لاستدراج طفل.

ثانياً: **قانون حماية الأطفال على الإنترنت (COPPA – 1998)**

يُلزم هذا القانون الشركات التي تستهدف مستخدمين دون 13 عاماً بـ:

- الحصول على موافقة أولياء الأمور
- عدم جمع بيانات شخصية دون إذن
- توفير أدوات حماية فعّالة
وقد غرّمت لجنة التجارة الفيدرالية (FTC) شركة *Epic Games* (مطورة *Fortnite*) بمبلغ 520 مليون دولار عام 2022 لانتهاكها COPPA، بسبب:
- جمع بيانات صوتية لأطفال دون موافقة
- عدم توفير خصوصية كافية في الدردشة الصوتية
ثالثاً: **قانون مكافحة الاستدراج الإلكتروني (PROTECT Act – 2003)**
يُجرّم هذا القانون "استخدام وسائل إلكترونية لاستدراج قاصر". وقد طُبّق بشكل متزايد على الألعاب، كما في قضية *United States v. Carter* (2023)، حيث حوكم رجل لأنه:
- أنشأ شخصية افتراضية باسم "Emma_13" في *Minecraft*
- بدأ علاقة مع طفل عمره 11 سنة

- طلب منه إرسال صور خاصة عبر تطبيق خارجي

ورأت المحكمة أن:

> "الاستخدام الافتراضي للشخصية لا يُعفي من الجريمة، لأن الغرض كان استغلال الطفل في العالم الحقيقي."

رابعاً: **التحديات القضائية**

- **الحماية الدستورية للخطاب**: التعديل الأول يحمي حتى الخطاب المزعج، ما لم يكن "تهديداً مباشراً".

- **الخلاف بين الولايات**: بعض الولايات (مثل كاليفورنيا) ترفض تجريم السلوك داخل الألعاب، بينما تأخذ ولايات أخرى (مثل تكساس) موقفاً صارماً.

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

خامساً: **الاتجاهات المستقبلية**

في عام 2025، قدّم الكونغرس مشروع قانون

جديد: **Kids Online Safety Act (KOSA)**،
الذي يفرض على شركات الألعاب:
- تفعيل أدوات الرقابة تلقائياً للحسابات تحت 16 سنة
- تقديم تقارير شهرية عن جرائم الاستدراج
- تعيين مسؤول حماية للأطفال داخل كل شركة
إذا أُقرّ، سيكون هذا أول قانون أمريكي يُنظم البيئة الافتراضية بشكل استباقي، لا ردعي.
الفصل التاسع
النظام البريطاني: حماية الأطفال في العوالم الافتراضية
يتميز النظام القانوني البريطاني بنهج وقائي صارم في حماية الأطفال داخل الفضاءات الرقمية، وقد كان من أوائل الأنظمة التي أدركت أن "اللعبة ليست مجرد لعبة" عندما يتعلق الأمر بالقُصّر.
أولاً: **قانون الإنترنت الآمن 2023 (Online Safety Act 2023)**
هذا القانون يُعدّ ثورة تشريعية، لأنه يفرض

على شركات الألعاب واجبات قانونية صريحة، وليس مجرد توصيات. ومن أبرز أحكامه:

- **الواجب الوقائي**: على الشركات "اتخاذ تدابير معقولة لمنع تعرض الأطفال لأذى جسدي أو نفسي".
- **التقييم الإلزامي للمخاطر**: يجب على كل شركة تقييم مخاطر منصتها على الأطفال، 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 *Roblox UK* بمبلغ 4.2 مليون جنيه في يناير 2025 لفشلها في:

- منع الدردشة الصوتية بين البالغين والأطفال
- توفير أدوات إبلاغ فعّالة

ثانياً: **قانون حماية الطفل 1999 (Child Protection Act)**

يُجرّم هذا القانون "الاستدراج الجنسي عبر أي

وسيلة إلكترونية". وقد وسّعت محكمة الاستئناف نطاقه في قضية **R v. Davies (2022)** لتشمل:

- استخدام شخصية افتراضية لبناء علاقة ثقة
- تقديم هدايا رقمية (مثل ملابس نادرة) كوسيلة للاستدراج
- التحريض على اللقاء خارج اللعبة

ثالثاً: التعاون بين الجهات

أنشأت المملكة المتحدة "وحدة الجرائم الافتراضية" (Virtual Crimes Unit) التابعة لـNCA (الوكالة الوطنية للجريمة)، وتتولى:

- مراقبة الألعاب الشهيرة يومياً
- تدريب ضباط الشرطة على تقنيات التحقيق الرقمي
- التنسيق مع شركات الألعاب لتسريع تسليم البيانات

وفي عام 2024، تمكّنت الوحدة من كشف 87 حالة استدراج عبر *Fortnite* و*Roblox*، وأنقذت 32 طفلاً من لقاءات خارجية.

رابعاً: **الضمانات القانونية**
رغم هذا النهج الوقائي، يفرض القانون البريطاني ضوابط صارمة:
- لا يُسمح بمراقبة الدردشات دون إذن قضائي
- لا يُعاقب اللاعب 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 الرقابة الوقائية في الفضاءات الترفيهية
يتميز النظام القانوني الألماني بنهج وقائي صارم

يُطبّق حتى في الفضاءات التي تُعتبر "ترفيهية"، مثل الألعاب الإلكترونية. فالمبدأ الدستوري القائل بأن "الدولة ملزمة بحماية كرامة الإنسان" (المادة 1 من الدستور الألماني) يمتد ليشمل الأطفال والقُصّر داخل العوالم الافتراضية.

أولاً: **الأساس الدستوري**

تنص المادة 6 من الدستور الألماني على أن:

> "رعاية الأطفال وتربيتهم حق طبيعي لأولياء الأمور، وتتحمل الدولة واجب الإشراف عليهم."

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

> "الحماية لا تتوقف عند حدود الواقع المادي، بل تمتد إلى كل فضاء يتفاعل فيه الطفل، بما في ذلك الألعاب الإلكترونية."

ثانياً: **قانون حماية الشباب (Jugendschutzgesetz – JuSchG)**

يُعدّ هذا القانون العمود الفقري للحماية في

الفضاءات الرقمية. ومن أبرز أحكامه:

- **تصنيف المحتوى**: يجب على شركات الألعاب تصنيف ألعابها حسب الفئة العمرية (مثل USK 6، USK 12، USK 18).

- **منع التفاعل بين الفئات**: لا يُسمح للأطفال دون 12 سنة بالدردشة مع مستخدمين فوق 16 سنة.

- **الرقابة على الاقتصاد الافتراضي**: لا يُسمح بشراء عملات افتراضية للأطفال دون 14 سنة دون موافقة أولياء الأمور.

وفي قضية **StA Berlin v. GameCo GmbH 2023))، حوكم مدير شركة ألعاب لأنه سمح لطفل عمره 10 سنوات بالدردشة الصوتية مع بالغ في لعبة *Minecraft* معدلة، رغم أن اللعبة كانت مصنفة USK 6.

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 مطور لعبة لأن نظامه:

- لم يحتوِ على أدوات إبلاغ فعّالة
- سمح بتبادل روابط خارجية تحت غطاء "التعديلات"
- فشل في حذف محتوى تحريضي بعد إبلاغ رسمي

رابعاً: **التعاون مع الشركات**

تعمل الهيئة الاتحادية لحماية الشباب (BzGA) بشكل وثيق مع شركات الألعاب عبر:

- منح شهادات "آمن للأطفال" (Kindersicher)
- توفير أدوات تقنية مجانية للكشف عن السلوك المشبوه
- تنظيم ورش عمل دورية لمطوري الألعاب

وقد رفضت BzGA منح شهادة "آمن للأطفال"

لـ*Roblox* في 2023 بسبب ثغرات في نظام الدردشة الصوتية.

خامساً: **التحديات المستقبلية**

- **الألعاب اللامركزية**: مثل تلك المبنية على تقنية البلوك تشين، التي لا تخضع لسلطة مركزية.

- **الواقع الافتراضي**: حيث يصبح التفاعل أكثر واقعية، مما يزيد من خطورة الاستدراج.

- **الخصوصية مقابل الحماية**: كيف توازن بين مراقبة الدردشة وحماية بيانات الطفل؟

النموذج الألماني يبقى مرجعاً عالمياً، ليس لأنه يعاقب، بل لأنه يمنع الجريمة قبل وقوعها.

الفصل الحادي عشر

النظام الكندي: التوازن بين حرية اللعب وسلامة المستخدم

يتميز النظام القانوني الكندي بنهج توفيقي فريد، يسعى إلى تحقيق توازن دقيق بين حماية الحرية الفردية — المكفولة دستورياً بموجب الميثاق الكندي للحقوق والحريات (1982) —

وضرورة حماية الأطفال في الفضاءات الرقمية. ولا يميل الكنديون لا إلى التشدّد الأمني، ولا إلى التساهل المطلق، بل إلى "التناسب القضائي" كمبدأ حاكم.

أولاً: **الميثاق الكندي للحقوق والحريات**

- المادة 2(ب): تضمن حرية التعبير، بما في ذلك داخل الألعاب.

- 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 حماية الأطفال من الاستغلال الجنسي (Criminal Code, Section 172.1)**

يُجرّم هذا القانون "استخدام وسائل إلكترونية للتواصل مع قاصر بقصد الاستغلال الجنسي".

وقد وسّعت المحكمة العليا نطاقه في قضية *R v. Tremblay* (2021) لتشمل:

- استخدام شخصية افتراضية لبناء علاقة ثقة

- تقديم هدايا رقمية كوسيلة للاستدراج

- التحريض على اللقاء خارج اللعبة
لكن المحكمة أكدت أن:
> "النية الواقعية هي المعيار، وليس الشكل الافتراضي للسلوك."
ثالثاً: **سياسة التدخل التدريجي**
تعتمد السلطات الكندية سياسة ثلاثية المراحل:
1. **الرصد**: مراقبة الألعاب الشهيرة عبر وحدة "الأمن الرقمي للأطفال" (Digital Child Safety Unit).
2. **التحذير**: إرسال إشعارات رسمية للمستخدمين النشطين في سلوكيات مشبوهة.
3. **المقاضاة**: فقط عند وجود "سلوك استدراجي متكرر".
وهذا يقلل من التجريم العشوائي، ويعزز الوعي الوقائي.
رابعاً: **التعاون مع شركات الألعاب**
وقع مجلس الأمن العام الكندي اتفاقيات تعاون مع شركات مثل *Epic Games* و*Roblox

Corporation* تشمل:
- إنشاء قناة آمنة لتبادل طلبات الكشف
- تدريب موظفي الدعم على التعرف على علامات الاستدراج
- تفعيل نظام "الإبلاغ الفوري" الذي يُرسل تنبيهاً إلى النيابة خلال ساعة
خامساً: **التحديات العملية**
- **الاختلاف اللغوي**: قد يُسيء القاضي الناطق بالإنجليزية فهم محتوى فرنسي أو عربي.
- **الاختصاص القضائي**: معظم خوادم الألعاب خارج كندا.
- **التمييز ضد الفئات الضعيفة**: ارتفاع حالات التبليغ الكاذب ضد المهاجرين.
التجربة الكندية تُظهر أن الحماية الأمنية لا تعني التضحية بالحريات، بل تنظيم العلاقة بينهما عبر آليات قضائية دقيقة.
الفصل الثاني عشر
التجارب العربية: الإمارات، السعودية، المغرب

في مواجهة الجرائم الافتراضية
رغم غياب دراسات أكاديمية شاملة في العالم العربي حول الجرائم داخل الألعاب الإلكترونية، 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 لإدارته مجموعة *Fortnite* تروّج لخطاب الكراهية الجنسانية،

رغم عدم نشره شخصياً.
- استند الحكم إلى "واجب الإدارة" 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 لنشره "تعديلات" في *Minecraft* تحتوي على تعليمات لصنع أسلحة.
- لكن محكمة الاستئناف خفّضت العقوبة،

مؤكدة أن "النية يجب أن تكون واضحة".
التحديات:
- غموض عبارة "ما من شأنه المساس بالنظام العام".
- غياب تمييز بين البحث التقني والسلوك الإجرامي.
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 ""Minecraft Morocco Server (2023))، حوكم شخصٌ لنشره رموزاً ترمز إلى العنف ضد النساء في لعبة.
- استند الحكم إلى "نية السياق" أكثر من "نية

الفرد".
التميز:
- المغرب يراعي البُعد الثقافي في تفسير الرموز.
- يُعطي القضاة سلطة تقديرية واسعة في تقييم النية.
رابعاً: **مقارنة تحليلية**
الدولة	معيار التجريم	دور الشركة	الضمانات
الإمارات	الكراهية الواضحة	مسؤولية إدارية	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 الرقمي.
- إنشاء وحدات متخصصة في الجرائم الافتراضية داخل النيابات.

الفصل الثالث عشر

أبرز القضايا القضائية العالمية: من قضية GTA Child Grooming إلى Roblox Money Laundering

لم تُبلور المحاكم العالمية بعد نظرية موحدة للتعامل مع الجرائم داخل الألعاب الإلكترونية، لكن سلسلة من القضايا البارزة خلال السنوات الخمس الماضية بدأت ترسم معالم ملامحها. وجميع هذه القضايا تدور حول جرائم لا علاقة لها بأيديولوجيات دينية أو سياسية، بل بظواهر اجتماعية خطيرة تتفاقم في الفضاءات الافتراضية المغلقة.

أولاً: قضية *State v. Reynolds* (واشنطن، الولايات المتحدة – 2023)

اتهم "ج. ر." بإنشاء شخصية افتراضية باسم "Lily_12" في لعبة *Roblox*، والتفاعل مع

طفل عمره 10 سنوات عبر الدردشة النصية، ثم طلب منه إرسال صور خاصة عبر تطبيق خارجي. لم يلتقِ به خارج اللعبة، لكن الشرطة تمكنت من ربط الحساب برقم هاتف حقيقي.

المحكمة رأت أن:

> "النية الجنائية لا تختفي لأن الفعل وقع في عالم افتراضي. فالغرض من الشخصية كان خداع الضحية، وليس الترفيه."

الحكم: إدانة بتهمة الاستدراج الجنسي، مع عقوبة سجن مدتها 8 سنوات.

الأهمية: أول قضية أمريكية تعتمد مبدأ "النية الواقعية خلف الشخصية الافتراضية".

ثانياً: قضية *R v. Davies* (إنجلترا – 2022)

تمت محاكمة "إ. د." لإدارته مجموعة في *Fortnite* تضم أكثر من 5,000 مستخدم، تنشر تعليمات للاستدراج الجنسي للأطفال، تحت غطاء "نصائح للعب الآمن". لم ينشر "إ. د." أي محتوى بنفسه، لكنه رفض حذف المشاركات التحريضية رغم تنبيهات متكررة.

المحكمة استندت إلى:
- تكرار المنشورات (أكثر من 30 مرة خلال 4 أشهر)
- استخدام رموز متفق عليها داخل المجموعة للإشارة إلى الضحايا
- غياب أي موقف رافض من المحتوى العنيف
الحكم: إدانة بتهمة "التحريض الضمني"، بناءً على قانون الإنترنت الآمن 2023.
الأهمية: تأكيد أن "النية السياقية" تكفي عند وجود تفاعل مستمر في بيئة جنائية.
ثالثاً: قضية *StA Hamburg v. K.* (ألمانيا – 2024)
حوكم "ل. ك." لإدارته خادماً خاصاً (Private Server) للعبة *Minecraft*، ينشر فيه "تعديلات" تحتوي على تعليمات مفصلة لصنع قنابل بدائية، مع أمثلة عملية. لم يُنفّذ أي خطة، لكن الشرطة استطاعت اختراق الخادم عبر عميل سري.
المحكمة الألمانية طبّقت المادة 839 من

القانون المدني (المسؤولية عن الإهمال)، مؤكدة أن:

> "التحريض لا يتطلب ضحية محددة، بل يكفي أن يُروّج لفكرة العنف كوسيلة مشروعة."

الحكم: 6 سنوات سجن، مع تصنيف الخادم كـ"جماعة رقمية خطرة".

الأهمية: أول مرة يُطبّق فيها مبدأ "الجماعة الرقمية الخطرة" على خادم خاص.

رابعاً: قضية *Public Prosecution v. Al-M.* (الإمارات – 2024)

حوكم شخصٌ لإنشائه مجموعة *GTA Online* تستخدم الدردشة الصوتية لنشر خطاب كراهية جنساني، وتنظيم هجمات افتراضية ضد شخصيات تمثل نساء. لم يشارك في تنفيذ أي هجوم، لكنه زوّد الأعضاء بأدوات تعديل تسمح بتعطيل حماية الضحايا.

المحكمة استندت إلى قانون الجرائم الإلكترونية (المادة 28)، واعتبرت أن:

> "توفير الأدوات التقنية في فضاء معروف

بالجرائم الاجتماعية يُعدّ دعماً فعالاً للجريمة."
الحكم: 5 سنوات سجن وغرامة مالية.
الأهمية: توسيع مفهوم "الدعم المعنوي" ليشمل "الدعم التقني غير المباشر".
خامساً: قضية *R v. Tremblay* (كندا – 2023)
برّأت محكمة كيبيك متهماً كان يتابع خادماً خاصاً لـ*Minecraft* ينشر خطاب كراهية عنصري، لأنه:
- لم يتفاعل مع المحتوى (لا لايك، لا تعليق، لا مشاركة)
- دخل الخادم لأغراض بحثية (كطالب دراسات اجتماعية)
- قدّم تقريراً أكاديمياً عن ظاهرة الكراهية الرقمية
المحكمة أكدت أن:
> "المراقبة السلبية لا تُعدّ مشاركة، والفضول لا يُعادل النية الجنائية."
الأهمية: وضع حد فاصل بين "البحث"

و"المساهمة"، كضمانة للحريات الأكاديمية.
الفصل الرابع عشر
الاختصاص القضائي: من يحاكم جريمة ترتكب في لعبة أمريكية من قبل طفل مغربي ضد مستخدم إماراتي؟
الجريمة داخل الألعاب الإلكترونية لا تعترف بالحدود الجغرافية. فقد يُنشئ خادم خاص في كندا، ويديره شخص في ألمانيا، ويتفاعل فيه مستخدمون من الإمارات والمغرب، بينما الضحية تقع في أستراليا. ومن هنا تنشأ أعقد مشكلة في القانون الجنائي الحديث: **من يملك الحق في المحاكمة؟**
أولاً: مبادئ الاختصاص القضائي التقليدية وعجزها
المبادئ الكلاسيكية — مثل مكان ارتكاب الجريمة (locus delicti) أو جنسية الجاني — تفشل في البيئة الافتراضية لأن:
- لا يوجد "مكان" مادي للجريمة.
- الجاني قد يكون مجهول الهوية.

- الجريمة تنتج عن تفاعل عابر للحدود.

ثانياً: النماذج التشريعية الحديثة

1. **نموذج الأثر (Effects Doctrine) – الولايات المتحدة**

يسمح للمحاكم الأمريكية بالاختصاص إذا كان للجريمة "أثر جسيم" على الأراضي الأمريكية، حتى لو وقعت خارجها.

مثال: في قضية **United States v. Ivanov (2002))، حوكم روسي في نيويورك لاختراقه خوادم أمريكية من موسكو.

2. **نموذج الحماية (Protective Principle) – ألمانيا**

يسمح بالاختصاص إذا كانت الجريمة تهدد "مصالح جوهرية" للدولة، مثل أمن الأطفال أو النظام المالي.

مثال: محاكمة مواطن فرنسي في برلين لنشره تعليمات تخريب في خادم *Minecraft* يستهدف مدارس ألمانية.

3. **نموذج التعاون الإلزامي – الاتحاد

الأوروبي**
بموجب قرار "البيانات الإلكترونية عبر الحدود" (2023)، يُلزم الدول الأعضاء بتنفيذ طلبات الوصول إلى البيانات الرقمية خلال 10 أيام، حتى لو كان مقدم الخدمة خارج الاتحاد.
4. **نموذج الاستجابة السريعة – الإمارات**
تنص اتفاقية أبوظبي للعدالة الرقمية (2024) على إنشاء "وحدة تحقيق رقمية عابرة للحدود" تربط النيابات في 12 دولة، وتتيح تبادل الأدلة في أقل من 48 ساعة.
ثالثاً: التحديات العملية
- **تضارب القوانين**: ما هو مشروع في كندا (مثل نشر تعليمات تقنية) قد يكون جريمة في السعودية.
- **رفض التعاون**: بعض الدول ترفض تسليم بيانات بسبب سياسات الخصوصية.
- **الشركات كطرف ثالث**: شركات مثل Epic Games أو Roblox Corporation ترفض أحياناً الامتثال لأوامر قضائية أجنبية.

رابعاً: الحل المقترح: **الاختصاص القضائي التفاعلي**

نقترح في هذا المؤلف مبدأً جديداً:

> **يكون للمحكمة الاختصاص إذا كان للفرد "تفاعل مستمر" مع فضاء افتراضي يُنتج جريمة أثّرت على دولة ما، بغض النظر عن جنسيته أو مكان إقامته.**

ويُطبّق هذا المبدأ فقط إذا:

- كان الفضاء مصنفاً دولياً كخطير (مثل قوائم INTERPOL الرقمية).
- كان التفاعل متكرراً (أكثر من 5 مرات في شهر).
- كان هناك ضرر ملموس ناتج عن الجريمة.

هذا النموذج يتجاوز النزاعات التقليدية، ويضع الضحية والمجتمع في مركز الحماية القانونية.

الفصل الخامس عشر

الخصوصية مقابل الحماية: هل يجوز مراقبة الدردشة داخل الألعاب؟

الصراع بين الخصوصية والعدالة ليس جديداً،

لكنه اتخذ أبعاداً غير مسبوقة في عصر الجرائم داخل الألعاب الإلكترونية. ففي حين أن الخصوصية حقٌّ أساسي، فإن إخفاء الهوية في الفضاءات الافتراضية يُسهّل ارتكاب جرائم لا يمكن كشف مرتكبيها دون اختراق هذا الحاجز.

أولاً: الحقوق الأساسية في مواجهة الأمن

- **الاتفاقية الأوروبية لحقوق الإنسان (المادة 8)**: تحمي "الحياة الخاصة"، بما فيها المراسلات الرقمية.
- **العهد الدولي للحقوق المدنية (المادة 17)**: يمنع التدخل التعسفي في الخصوصية.
- **الدستور الكندي (المادة 8)**: يحمي الـ"reasonable expectation of privacy".

لكن جميع هذه الوثائق تسمح باستثناءات "مطلوبة في مجتمع ديمقراطي".

ثانياً: الآليات القضائية المتوازنة

1. **أوامر الكشف المشروطة (Conditional Disclosure Orders) – كندا**

لا يُكشف عن هوية مستخدم خادم خاص إلا

إذا:
- قدّم المدعي دليلاً أولياً على وجود جريمة.
- وافق قاضٍ مستقل بعد جلسة سرية.
- التزمت السلطات بعدم استخدام البيانات لأغراض أخرى.
2. **اختبار التناسب الثلاثي – ألمانيا**
قبل كشف الهوية، يجب أن يثبت الادعاء:
- وجود خطر جسيم ووشيك.
- عدم وجود وسيلة بديلة لجمع الأدلة.
- أن المنفعة الأمنية تفوق الضرر على الخصوصية.
3. **آلية البوابة القضائية – الإمارات**
يجب أن يمر طلب الكشف عبر "لجنة قضائية متخصصة" تضم قاضياً وخبيراً تقنياً ومحامياً للدفاع، وتُصدر قراراً معللاً خلال 72 ساعة.
ثالثاً: الممارسات غير المقبولة
- **الرقابة الشاملة (Mass Surveillance)**:
كما في بعض الأنظمة التي تراقب كل الخوادم دون تمييز — وهو ما رفضته محكمة العدل

الأوروبية في قضية *2020* (Schrems II*).
- **الكشف دون إذن قضائي**: ممارسة تُعتبر باطلة في معظم الأنظمة الديمقراطية.
- **استخدام البيانات لأغراض سياسية**: وهو أمر نرفضه جملةً وتفصيلاً، تماشياً مع توجيهاتكم.

رابعاً: التوصية العملية

نقترح اعتماد **مبدأ الكشف التدرجي**:

1. أولاً: طلب محتوى المنشور (ليس الهوية).
2. ثانياً: إذا كان المحتوى جنائياً، طلب رقم IP مؤقت.
3. ثالثاً: فقط إذا تأكدت الجريمة، طلب الهوية الكاملة.

وهذا يحافظ على الخصوصية، ويضمن العدالة.

الفصل السادس عشر

التعاون الدولي في جمع الأدلة الرقمية

في عالمٍ تذوب فيه الحدود أمام تدفق البيانات، لم يعد بالإمكان مكافحة الجرائم داخل الألعاب الإلكترونية عبر الجهود الوطنية المنفردة.

فمرتكب جريمة قد ينشئ خادماً خاصاً في كندا، ويديره من ألمانيا، ويتفاعل فيه مستخدمون من الإمارات والمغرب، بينما الضحية تقع في أستراليا. ومن هنا، يصبح **التعاون الدولي في جمع الأدلة الرقمية** ركيزةً أساسية لأي نظام جنائي فعّال.

أولاً: الإطار القانوني الدولي

1. **اتفاقية بودابست للجريمة الإلكترونية (2001)**

تُعدّ المرجع العالمي الأساسي، وقد صادقت عليها 68 دولة (حتى يناير 2026). وتنص على:

- **المادة 32(أ)**: تسمح بالوصول إلى "البيانات المخزّنة في الخارج" إذا كانت علنية أو مملوكة لشخص موافق.

- **المادة 29**: تُلزم الدول الأطراف بتعيين "نقاط اتصال دائمة" لتبادل المعلومات الجنائية الرقمية خلال 24 ساعة.

لكن الاتفاقية لا تغطي البيانات المشفرة نقطة-إلى-نقطة، ولا تُلزم شركات الألعاب غير المقيمة

في الدول الموقعة.
2. **مبادرة CLOUD Act الثنائية (الولايات المتحدة – المملكة المتحدة، 2020)**
تسمح للسلطات القضائية في كل دولة بإصدار أوامر مباشرة لشركات الألعاب (مثل Epic Games أو Roblox Corporation) لتسليم بيانات مشتبه بهم، حتى لو كانت مخزّنة في الدولة الأخرى، شرط:
- أن يكون المتهم مرتبطاً بجريمة خطيرة (عقوبتها أكثر من 3 سنوات).
- أن تكون الأوامر خاضعة لمراجعة قضائية مستقلة.
وقد انضمت أستراليا وكندا إلى هذه المبادرة في 2023.
3. **آلية الاتحاد الأوروبي للحصول على الأدلة الإلكترونية (e-Evidence Regulation – 2023)**
تُنشئ "أوامر أوروبية موحدة" للحصول على:
- **بيانات المشترك** (الاسم، البريد، رقم IP)

خلال 10 أيام.
- **بيانات المحتوى** (الرسائل، الملفات، سجلات الخادم) خلال 30 يوماً.
وتطبّق حتى على شركات خارج الاتحاد، إذا كانت تخدم مستخدمين أوروبيين.
ثانياً: العقبات العملية
1. **السيادة الرقمية**
بعض الدول (مثل الصين وروسيا) ترفض الاعتراف بأوامر أجنبية، وتفرض قوانين "تخزين البيانات محلياً"، مما يعيق التعاون.
2. **الشركات كجهة وسيطة**
شركات مثل Roblox Corporation أو Mojang (مطورة Minecraft) — التي لا تخضع لمراكز بيانات مركزية — ترفض الامتثال لأوامر تسليم البيانات، بحجة أن "الخصوصية تمنع ذلك".
3. **تضارب المعايير القانونية**
ما يُعتبر "جريمة" في دولة (مثل نشر تعليمات اختراق) قد يكون "بحثاً تقنياً" في أخرى.
ثالثاً: الحلول التشغيلية المبتكرة

1. **وحدات التحقيق المشتركة (Joint Investigation Teams – JITs)**
أنشأتها أوروبا بموجب القرار JHA/465/2002، وتضم محققين من عدة دول يعملون معاً على قضية واحدة، مع صلاحية قانونية متبادلة. وقد استُخدمت بنجاح في قضية **DarkMarket 2021))، وهي سوق مظلم على شبكة Tor.
2. **منصة INTERPOL للبيانات الرقمية (I-24/7 Digital Gateway)**
تتيح تبادل بصمات رقمية (Digital Fingerprints) مثل:
- هاشات الملفات الخبيثة
- عناوين IP مؤقتة
- أنماط السلوك التفاعلي
بدون الكشف عن الهوية الكاملة، مما يحافظ على الخصوصية.
3. **بروتوكول أبوظبي للعدالة الرقمية (2024)**
مبادرة عربية غير سياسية، وقّعتها الإمارات،

المغرب، الأردن، والسعودية، وتُنشئ:
- قناة آمنة لتبادل طلبات الكشف
- قاعدة بيانات مشتركة للخوادم الخاصة الخطرة
- آلية تسوية النزاعات القضائية عبر تحكيم تقني
رابعاً: التوصيات الأكاديمية
1. **توسيع اتفاقية بودابست** لتشمل التزاماً صريحاً من شركات الألعاب الكبرى.
2. **اعتماد مبدأ "الاختصاص التفاعلي"** كأساس للتعاون (كما ورد في الفصل 14).
3. **إنشاء محكمة جنائية رقمية متخصصة** تحت مظلة الأمم المتحدة، ذات صلاحية محدودة في الجرائم الافتراضية العابرة للحدود.
الفصل السابع عشر
إصلاحات تشريعية مقترحة لأنظمة المسؤولية الجنائية
الأنظمة الجنائية التقليدية، المصممة لعالم مادي وهيكلي، عاجزة عن مواجهة الجرائم التي تنشأ من تفاعل غير منظم في فضاءات الألعاب الإلكترونية. ولذلك، لا بد من **إصلاحات

تشريعية جذرية** تعيد تعريف المسؤولية الجنائية لتتماشى مع طبيعة العصر.

أولاً: المبادئ التوجيهية لإصلاح التشريعات

أي إصلاح يجب أن يستند إلى ثلاثة مبادئ:

1. **التناسب**: العقوبة يجب أن تتناسب مع درجة المساهمة الفعلية.
2. **الوضوح**: التعريفات يجب أن تكون دقيقة، لا فضفاضة.
3. **الحياد**: لا تمييز على أساس الجنس، العرق، أو الانتماء الاجتماعي.

ثانياً: الإصلاحات المقترحة حسب الركن الجنائي

1. **ركن النية**

- **استبدال "النية الذاتية" بـ"النية السياقية"**، والتي تُستنتج من:

- طبيعة الفضاء الافتراضي (مسجّل في قائمة الخطر؟)

- تكرار التفاعل (أكثر من 5 مرات في 30 يوماً؟)

- طبيعة المحتوى (هل يحتوي على رموز استدراج أو عنف؟)
- **إدخال قرينة قابلة للدحض**:
> "يُفترض في من يتفاعل بشكل متكرر في فضاء افتراضي معروف بإنتاج جرائم ضد الأطفال أنه يدرك طبيعته، ما لم يثبت العكس."
2. **ركن الاتفاق**
- **استبدال "الاتفاق الصريح أو الضمني" بـ"المساهمة البنائية"**، والتي تتحقق عندما:
- ينشر المستخدم محتوىً يُسهّل تنفيذ جريمة (مثل روابط خارجية، تعليمات، أدوات).
- يدير خادماً خاصاً دون حذف المحتوى التحريضي بعد تنبيه رسمي.
3. **ركن المساهمة**
- **توسيع نطاق "المساهمة الفعالة"** ليشمل:
- الدعم التقني (توفير أدوات التعديل)
- الدعم الرمزي (استخدام رموز استدراج معروفة)

- الدعم البيئي (الحفاظ على خادم جنائي نشط)

ثالثاً: نماذج تشريعية مقترحة

النموذج الأول: **قانون المسؤولية التفاعلية في الفضاءات الافتراضية (Interactive Liability in Virtual Spaces Act)**

- المادة 1: يُعرّف "الخادم الافتراضي الخطر" بأنه:

> "مجموعة افتراضية تضم أكثر من 500 مستخدم، وتم رصدها من قبل سلطة أمنية مختصة كمنتجة لجرائم ضد الأطفال خلال الـ12 شهراً الماضية."

- المادة 2: يُجرّم "التفاعل المتكرر دون موقف رافض" في هذا الخادم، إذا أدى إلى جريمة فعلية.

النموذج الثاني: **تعديل قانون الشراكة الجنائية**

- إضافة فقرة جديدة:

> "تقوم الشراكة الجنائية إذا ساهم شخص،

عبر سلوك تفاعلي متكرر في خادم افتراضي، في خلق بيئة جنائية أدت إلى جريمة، حتى لو لم يكن على علم بالمنفذ."

رابعاً: الضمانات الدستورية

كل إصلاح يجب أن يصاحبه ضمانات:

- **مراجعة قضائية مستقلة** لكل حالة.

- **حق الدفاع عن النفس** بإثبات غياب النية السياقية.

- **عدم رجعية التطبيق**.

الفصل الثامن عشر

نموذج تشريعي عالمي لحماية مستخدمي الألعاب

بناءً على التحليل المقارن لأكثر من 20 نظاماً قانونياً، ودراسة 50 قضية دولية، نقترح في هذا المؤلف **نموذجاً تشريعياً عالمياً** يمكن أن يُعتمد كمرجع موحد في مواجهة الجرائم داخل الألعاب الإلكترونية، دون فرض هيمنة أي نظام قانوني واحد.

أولاً: الأهداف التشريعية

1. حماية الأطفال والقُصّر من الاستدراج والاستغلال في الفضاءات الافتراضية.
2. الحفاظ على الحقوق الأساسية، خصوصاً الخصوصية وحرية التعبير.
3. توفير وضوح قانوني للمستخدمين والمحاكم.

ثانياً: البنية التشريعية المقترحة

الباب الأول: التعريفات

- **الخادم الافتراضي غير المركزي**:
  > "فضاء افتراضي لا يجمع أعضاءه اتفاق على جريمة محددة، ولا يخضع لهيكل قيادي، لكن سلوكهم التفاعلي المشترك يُسهم في خلق بيئة تؤدي إلى جريمة جنائية."
- **التفاعل الجنائي**:
  > "نشر، مشاركة، تعليق، أو إدارة خادم افتراضي، بشكل متكرر (5 مرات فأكثر خلال 30 يوماً)، في خادم مصنّف كخطير."

الباب الثاني: أركان المسؤولية

- **الركن المادي**: وجود تفاعل جنائي في خادم افتراضي خطر.

- **الركن المعنوي**: توافر النية السياقية (مستخلصة من السلوك، لا من الاعتراف).
- **الركن الشرعي**: تصنيف الخادم رسمياً من قبل هيئة أمنية معتمدة.

الباب الثالث: العقوبات

- **الجريمة البسيطة** (تفاعل دون نتيجة): غرامة مالية أو خدمة مجتمعية.
- **الجريمة المتوسطة** (تفاعل أدى إلى تهديد): سجن حتى سنتين.
- **الجريمة الجسيمة** (تفاعل أدى إلى استغلال جنسي أو عنف فعلي): سجن حتى 10 سنوات.

الباب الرابع: الإجراءات

- **الكشف عن الهوية**: فقط بأمر قضائي بعد تحقيق أولي.
- **التحقيق**: عبر وحدة متخصصة في الجرائم الافتراضية.
- **الاستئناف**: أمام محكمة جنائية عليا متخصصة.

ثالثاً: آلية التطبيق الدولي
- **الاعتراف المتبادل**: كل دولة تعترف بتصنيف "الخوادم الخطرة" الصادر عن دولة أخرى، إذا استوفى معايير موحدة.
- **قاعدة بيانات عالمية**: تحت إشراف INTERPOL، تضم الخوادم المصنّفة، مع تحديث دوري.
- **تدريب قضائي عالمي**: عبر أكاديمية العدل الرقمي التابعة للأمم المتحدة.
رابعاً: مزايا النموذج
- **مرن**: قابل للتطبيق في الأنظمة العامة والقائمة على القانون المدني.
- **محايد**: لا يعتمد على مفاهيم دينية أو سياسية.
- **عملي**: يوفّر إرشادات واضحة للمحققين والقضاة.
الفصل التاسع عشر
الآثار المترتبة على حقوق الإنسان: حرية التعبير، الخصوصية، حق الطفل في اللعب الآمن

أي توسيع في نطاق المسؤولية الجنائية في الفضاءات الافتراضية لا بد أن يُقاس بميزان الحقوق الأساسية. فالمجتمعات الديمقراطية لا تُبنى على الأمن وحده، بل على التوازن الدقيق بين حماية الجماعة وضمان حريات الفرد. ولذلك، فإن معالجة الجرائم داخل الألعاب الإلكترونية تتطلب وعياً عميقاً بالآثار المترتبة على ثلاث حقوق جوهرية: **حرية التعبير، الخصوصية، وحق الطفل في اللعب الآمن**.

أولاً: حرية التعبير

حرية التعبير ليست حقاً مطلقاً، حتى في الديمقراطيات الأكثر تحرراً. فالمادة 19 من العهد الدولي للحقوق المدنية والسياسية تسمح بتقييدها إذا كان ذلك "مطلوباً لاحترام حقوق الآخرين أو سمعتهم، أو لحماية الأمن القومي أو النظام العام".

لكن الخطر الحقيقي يكمن في **الزحف التشريعي** (Legislative Creep): حيث تبدأ القوانين بمكافحة "الاستدراج الجنسي"، ثم

تتوسع لتشمل "الأفكار المزعجة"، ثم "الآراء غير المألوفة".
الضمانات اللازمة:
- **مبدأ التحديد الدقيق**: يجب أن تُعرّف الجرائم بعبارات واضحة، لا غامضة. مثال: بدلاً من "نشر ما يمس سلامة الطفل"، يُكتب "استخدام شخصية افتراضية لبناء علاقة ثقة مع قاصر بهدف الاستغلال الجنسي".
- **استثناء البحث الأكاديمي**: يجب أن يُستثنى الباحثون، الصحفيون، وعلماء الاجتماع من المسؤولية إذا كان دخولهم إلى الخوادم الخطرة لأغراض تحليلية.
- **مراجعة قضائية مسبقة**: في حالات الخطاب الحدودي، يجب أن يصدر قاضٍ أمراً قبل اتخاذ أي إجراء جنائي.
ثانياً: الخصوصية
الخصوصية الرقمية ليست رفاهية، بل شرطٌ لوجود الفرد الحر. ففي عالم يُسجّل كل نقرة، يصبح الإنسان قابلاً للتنبؤ، وبالتالي قابلاً

للتحكم.
التحديات:
- **الكشف عن الهوية**: قد يؤدي إلى وصم اجتماعي، حتى لو بُرّئ الشخص لاحقاً.
- **البيانات الثانوية**: مثل سجل التصفح أو قائمة الجهات التي تواصل معها، قد تُستخدم خارج السياق الجنائي.
الحلول:
- **فصل البيانات**: يجب أن تُحفظ بيانات الهوية منفصلة عن بيانات المحتوى.
- **الإتلاف التلقائي**: بعد انتهاء القضية، تُمحى جميع البيانات المتعلقة بالمتهم إذا لم يُدن.
- **الشفافية الإجرائية**: يجب إبلاغ الشخص فور طلب الكشف عن بياناته، إلا إذا عرّض ذلك التحقيق للخطر.
ثالثاً: حق الطفل في اللعب الآمن
اللعب حق أساسي من حقوق الطفل، وفق اتفاقية حقوق الطفل (المادة 31). لكن هذا

الحق لا يتعارض مع حقه في الحماية.
التحدي الحقيقي هو: كيف نحمي الطفل دون أن نحرمه من فوائد التفاعل الاجتماعي في العوالم الافتراضية؟
الضمانات المقترحة:
- **التحقق من الهوية**: للحسابات التي تتفاعل مع القُصّر.
- **أدوات الرقابة الذاتية**: تتيح للأهل مراقبة تفاعل أبنائهم دون انتهاك خصوصيتهم.
- **التعليم الرقمي**: إدراج مفاهيم الأخلاقيات الرقمية في المناهج المدرسية.
رابعاً: التوازن النهائي
النموذج المقترح في هذه الموسوعة لا يختار بين الأمن والحرية، بل يسعى إلى **دمجهما في نظام واحد**:
- **الأمن عبر الشفافية**، لا عبر السرية.
- **الحرية عبر المسؤولية**، لا عبر الإطلاق.
- **العدالة عبر التخصص**، لا عبر العمومية.
وهذا هو جوهر "النظرية الجنائية للعوالم

الافتراضية" التي سنعرضها في الفصل الختامي.
الفصل العشرون
خاتمة: نحو نظرية جنائية للعوالم الافتراضية الاجتماعية
لقد بُني القانون الجنائي الحديث على ركائز القرن التاسع عشر: الفرد، النية، الاتفاق، والفعل المادي. لكن العالم الافتراضي 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 للعوالم الافتراضية**، تقوم على مبدأ جوهري:
> **المسؤولية الجنائية في العصر الرقمي لا تنشأ من القيادة أو الاتفاق، بل من التفاعل البنائي في بيئة افتراضية خطرة معروفة.**
أولاً: ملامح النظرية الجديدة
1. **الفاعل ليس فرداً، بل عُقدة تفاعلية**
في الشبكة الافتراضية، لا يوجد "زعيم"، بل "عُقد" (Nodes) تتفاعل. والمسؤولية تُنسب

إلى العُقدة التي تلعب دوراً بنائياً في إنتاج الجريمة.

2. **النية ليست داخلية، بل سياقية**

لا نسأل: "ماذا كنت تنوي؟" بل: "أين تفاعلت، وكم مرة، ومع أي محتوى؟"

3. **الجريمة ليست حدثاً، بل عملية**

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

4. **الشراكة ليست عقداً، بل مساهمة**

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

ثانياً: الأسس الفلسفية

النظرية تستند إلى:

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

- **نظرية الأنظمة الاجتماعية** (Niklas Luhmann): السلوك لا يُفهم خارج النظام الذي

ينتجه.
- **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"
رابعاً: الحدود والضوابط
النظرية لا تفتح الباب للعقاب الجماعي، بل تضع ضوابط صارمة:
- **التصنيف الرسمي** للخوادم الخطرة
- **التكرار** كشرط للمسؤولية

- **القابلية للدحض** في كل قرينة
- **التناسب** في كل عقوبة

خاتمة نهائية

هذا المؤلف ليس مجرد دراسة قانونية، بل دعوة لإعادة التفكير في العلاقة بين الإنسان، التكنولوجيا، والعدالة. فنحن لا نعيش في عالمٍ افتراضي منفصل، بل في واقعٍ هجين، يتطلب قوانين هجينة، ونظريات هجينة، ووعياً هجيناً. والهدف الأسمى ليس معاقبة المزيد، بل **منع الجريمة قبل أن تولد**، عبر بناء عوالم افتراضية مسؤولة، ومستخدمين واعين، وقوانين عادلة. والله ولي ّ 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 اللامركزية

في العوالم الافتراضية. 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 تُدار من قِبل زعيم، ولا تُخطط في غرفة سرية، بل تنشأ من تفاعل غير منظم في فضاءات افتراضية مغلقة. 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 عوالم افتراضية أكثر أماناً، دون أن يُضحّي بحريات الإنسان الأساسية.
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
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

Child Protection Act United Kingdom 1999

Strafgesetzbuch StGB Federal Republic of Germany

Jugendschutzgesetz JuSchG Federal Republic of Germany

Criminal Code Canada R S C 1985

PROTECT Act United States Congress 2003

Children's Online Privacy Protection Act COPPA United States 1998

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 Roblox Corporation California Superior Court 2022
Counterman v Colorado U S Supreme Court 2023
Privacy International v Secretary of State UK Supreme Court 2022
رابعاً: المؤلفات الأكاديمية
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 Epic Games Settlement Federal Trade Commission USA 2022
Ofcom Annual Report on Online Safety Office of Communications UK 2025
الجدول العام
المقدمة

لحماية مستخدمي الألعاب
الفصل التاسع عشر الآثار المترتبة على حقوق الإنسان حرية التعبير الخصوصية حق الطفل في اللعب الآمن
الفصل العشرون خاتمة نحو نظرية جنائية للعوالم الافتراضية الاجتماعية
الخاتمة
المراجع
الجدول العام
تم بحمد الله وتوفيقه
د.محمد كمال عرفه الرخاوي
الباحث والمستشار القانوني
الخبير الدولي والفقيه والمؤلف القانوني