اتفاقية بودابست بشأن الجريمة السيبرانية - مرجع عربي



اتفاقية بودابست بشأن الجريمة السيبرانية

عندما تعبر الأدلة الرقمية الحدود

دراسة تعريفية تحليلية في التعاون الدولي والحصول على الأدلة الإلكترونية، مع قراءة في فرص الاستفادة والتحديات بالنسبة للسودان

إعداد: آدم السنوسي آدم عثمان
وكيل نيابة مكافحة جرائم المعلوماتية

حالة المعلومات الدولية: سبتمبر 2026

تنبيه منهجي

تعتمد هذه الدراسة في عرض اتفاقية بودابست وبروتوكوليها على المصادر الرسمية لمجلس أوروبا. أما ما يتعلق بالسودان فيجب قراءته في ضوء النصوص السودانية النافذة وتعديلاتها والممارسة الإجرائية حتى تاريخ الدراسة. ولا تعني الإشارة إلى معيار أو آلية دولية أنها نافذة تلقائياً في السودان ما لم يوجد الأساس القانوني الذي يجعلها كذلك.

الورقة تحليلية وتعريفية؛ ولا تفترض أن الانضمام إلى الاتفاقية هو الخيار الأفضل أو الأسوأ للسودان.

الملخص التنفيذي

تتناول هذه الورقة اتفاقية بودابست بشأن الجريمة السيبرانية باعتبارها إطاراً دولياً للتجريم والإجراءات المتعلقة بالأدلة الإلكترونية والتعاون العابر للحدود. وتشرح نشأة الاتفاقية، سلطات حفظ البيانات والبحث والضبط، شبكة الاتصال 24/7، البروتوكولين الإضافيين، والتعاون مع مزودي الخدمات.

كما تقدم قراءة من منظور سوداني، مع التمييز بين التقارب في بعض صور التجريم وبين الحاجة إلى فحص أعمق للأدوات الإجرائية والتعاون الدولي والضمانات المتعلقة بالسيادة والخصوصية وحماية البيانات.

ويمتد التحليل إلى التحقيق المالي في الجرائم السيبرانية ذات العائد المالي، مع توضيح أن بودابست ليست اتفاقية مستقلة لاسترداد الأموال، وأن تتبع العائدات وتجميدها ومصادرتها واستردادها يتكامل مع قوانين وآليات مكافحة غسل الأموال واسترداد الأصول، ومنها اتفاقية وارسو CETS 198 ومشروعات عملية مثل iPROCEEDS.

الفهرس

- 1. مقدمة الدراسة
- 2. نشأة اتفاقية بودابست وطبيعتها القانونية
- 3. نطاق التجريم
- 4. الإجراءات والأدلة الإلكترونية
- 5. التعاون الدولي وشبكة 24/7
- 6. البروتوكول الإضافي الأول
- 7. البروتوكول الإضافي الثاني ومزودو الخدمات
- 8. السودان واتفاقية بودابست
- 9. السيادة والخصوصية والتحفظات القانونية
- 10. من الدليل الإلكتروني إلى تتبع عائدات الجريمة
- 11. نموذج عملي للتحقيق السيبراني المالي
- 12. النتائج
- 13. التوصيات
- 14. الخاتمة
- 15. أهم المصطلحات
- 16. المراجع الرسمية

1. مقدمة الدراسة

أصبحت الأدلة الرقمية عابرة للحدود بطبيعتها. فقد تقع الجريمة في دولة، ويكون المجني عليه في دولة ثانية، ويستخدم الجاني منصة تديرها شركة في دولة ثالثة، بينما تحفظ البيانات في بنية تقنية موزعة دولياً. لذلك لم يعد السؤال فقط: من ارتكب الجريمة؟ بل أيضاً: أين يوجد الدليل؟ من يحوزه؟ كيف يُحفظ قبل أن يزول؟ وما الطريق القانوني للحصول عليه؟

جاءت اتفاقية بودابست بشأن الجريمة السيبرانية ETS No.185 لتضع إطاراً مشتركاً في ثلاثة محاور: حد أدنى من التجريم، سلطات إجرائية للتعامل مع الأدلة الإلكترونية، وآليات للتعاون الدولي.

الجريمة قد تكون تقليدية، لكن الدليل قد يكون رقمياً.

2. نشأة الاتفاقية وطبيعتها القانونية

فُتحت الاتفاقية للتوقيع في بودابست في 23 نوفمبر 2001، ودخلت حيز النفاذ في 1 يوليو 2004. وهي معاهدة لمجلس أوروبا، وليست تشريعاً للاتحاد الأوروبي. كما أن نظامها يسمح بانضمام دول من خارج أوروبا وفق الإجراءات المنصوص عليها في الاتفاقية.

حتى سبتمبر 2026 يظهر سجل المعاهدات الرسمي اتساع نطاق المشاركة في الاتفاقية عالمياً، وهو ما يعكس تحولها إلى أحد أهم الأطر الدولية المستخدمة في مجال الجريمة السيبرانية والأدلة الإلكترونية.

3. نطاق التجريم

تتناول المواد الموضوعية الأساسية صوراً من الاعتداء على سرية وسلامة وتوافر البيانات والأنظمة، إضافة إلى جرائم تعتمد الحاسوب كوسيلة.

- الدخول غير المشروع إلى أنظمة الحاسوب - المادة 2.
- الاعتراض غير المشروع للبيانات - المادة 3.
- التدخل في البيانات - المادة 4.
- التدخل في الأنظمة - المادة 5.
- إساءة استخدام الأجهزة والبرامج وكلمات المرور في الحالات التي تغطيها المادة 6.
- التزوير المرتبط بالحاسوب - المادة 7.
- الاحتيال المرتبط بالحاسوب - المادة 8.
- جرائم أخرى تناولتها الاتفاقية، إلى جانب المسؤولية والمحاولة والمساعدة والعقوبات وفق نطاقها.

القيمة المقارنة بالنسبة للسودان لا تتمثل في البحث عن تطابق لفظي بين النصوص فقط، بل في مقارنة نطاق التجريم والعناصر المادية والمعنوية والاختصاص والجزاءات والضمانات.

4. الإجراءات والأدلة الإلكترونية

من أهم ما يميز بودابست أنها لا تقف عند التجريم. المواد 16-21 تقدم مجموعة من الأدوات الإجرائية التي تتعامل مع الطبيعة السريعة الزوال للبيانات.

- المادة 16: الحفظ العاجل للبيانات المخزنة.
- المادة 17: الحفظ العاجل والكشف الجزئي عن بيانات المرور.
- المادة 18: أمر تقديم البيانات.
- المادة 19: البحث والوصول والضبط بالنسبة للبيانات المخزنة.
- المادة 20: الجمع الآني لبيانات المرور.

• المادة 21: اعتراض بيانات المحتوى في الحدود التي يقررها القانون.

الحفظ لا يعني الإفصاح، والإفصاح لا يعني قبول الدليل تلقائياً أمام المحكمة.

وتؤكد المادة 15 أهمية الشروط والضمانات وحماية حقوق الإنسان ومبدأ التناسب. لذلك لا ينبغي قراءة سلطات التحقيق منفصلة عن القيود القانونية المصاحبة لها.

5. التعاون الدولي وشبكة 24/7

ينظم الفصل الثالث من الاتفاقية التعاون الدولي في الجرائم السيبرانية والأدلة الإلكترونية. وتشمل المنظومة المساعدة القانونية المتبادلة والحفظ العاجل والتعاون بشأن الوصول إلى البيانات المخزنة وغيرها من الأدوات.

وتنشئ المادة 35 شبكة نقاط اتصال تعمل على مدار 24 ساعة طوال أيام الأسبوع لتقديم المساعدة الفورية في التحقيقات المتعلقة بالأنظمة والبيانات أو جمع الأدلة الإلكترونية.

شبكة 24/7 ليست جهة دولية تصدر أوامر قبض أو تجميد أموال؛ بل شبكة نقاط اتصال وطنية لتسريع المساعدة والتعاون.

المادة 32 والوصول العابر للحدود

تتناول المادة 32 حالتين محدودتين للوصول العابر للحدود دون الحصول على إذن منفصل من دولة أخرى: البيانات المتاحة للعامة، والوصول إلى بيانات موجودة في دولة أخرى بموافقة قانونية وطوعية ممن يملك سلطة قانونية على الإفصاح. ولهذا تظل المادة من أكثر مواد الاتفاقية حساسية من زاوية السيادة والاختصاص.

6. البروتوكول الإضافي الأول

فُتح البروتوكول الإضافي الأول للتوقيع في 28 يناير 2003، ويتعلق بتجريم أفعال ذات طبيعة عنصرية وكراهية الأجانب تُرتكب من خلال أنظمة الحاسوب. وهو أداة مستقلة عن نص الاتفاقية الأصلية من حيث الالتزامات التي يضيفها.

7. البروتوكول الإضافي الثاني ومزودو الخدمات

فُتح البروتوكول الإضافي الثاني CETS No.224 للتوقيع في 12 مايو 2022، ويهدف إلى تعزيز التعاون والإفصاح عن الأدلة الإلكترونية. ويقدم آليات تتعلق بمعلومات تسجيل أسماء النطاقات، ومعلومات المشتركين، والتعاون الحكومي المعجل، وحالات الطوارئ، والتحقيقات المشتركة والمؤتمرات المرئية، مع ضمانات لحماية البيانات وحقوق الإنسان.

حتى سبتمبر 2026، يبين سجل المعاهدات الرسمي أن دخوله حيز النفاذ يتطلب خمس تصديقات، ولم يكن هذا الشرط قد اكتمل بعد؛ لذلك لا توصف أحكامه في هذه الورقة بأنها نافذة دولياً في ذلك التاريخ.

مزود الخدمة قد يكون حائزاً للدليل الرقمي، لكنه لا يمنح سلطات التحقيق وصولاً مفتوحاً إلى قواعد بياناته.

يمكن استخدام Meta أو Microsoft أو Google كأمثلة لمزودي خدمات عالميين قد تكون لديهم بيانات مرتبطة بتحقيق ما، لكن البروتوكول لا ينشئ امتيازاً خاصاً تجاه شركة بعينها ولا يساوي بين معلومات المشترك وبيانات المرور ومحتوى الاتصالات.

8. السودان واتفاقية بودابست

السودان ليس طرفاً في اتفاقية بودابست حالياً. ولذلك لا تنشأ للسلطات السودانية تلقائياً الحقوق والآليات المقررة للدول الأطراف لمجرد أن الدليل موجود لدى مزود خدمة في دولة طرف.

مع ذلك، تمثل الاتفاقية معياراً مقارناً مفيداً عند تقييم كفاية التشريع والممارسة الوطنية في أربعة مجالات: التجريم، الحفظ العاجل للأدلة، سلطات الحصول على البيانات، والتعاون الدولي.

يظهر في قانون مكافحة جرائم المعلوماتية السوداني لسنة 2018 تقارب في عدد من صور التجريم، لكن الحكم على التطابق الكامل يحتاج إلى قراءة القانون مع قانون الإجراءات الجنائية والتعديلات اللاحقة والتشريعات ذات الصلة والممارسة العملية.

السؤال المقارن ليس: هل عندنا جريمة اسمها الاختراق؟ بل: هل نملك أيضاً الأدوات القانونية لحفظ الدليل الموجود بالخارج والحصول عليه في الوقت المناسب؟

9. السيادة والخصوصية والتحفظات القانونية

تثير منظومة التعاون العابر للحدود أسئلة قانونية مشروعة. أبرزها حدود السيادة والاختصاص، وحماية البيانات الشخصية، والتناسب، والرقابة القضائية أو المستقلة، والعلاقة بين السلطات الوطنية ومزودي الخدمات الأجانب.

- السيادة: متى يجوز الوصول إلى بيانات تقع خارج الإقليم، ومن يملك الإذن؟
- الخصوصية: ما الحد الأدنى الضروري من البيانات المطلوب نقله؟
- الاختصاص: أي قانون يحكم الطلب والتنفيذ وحجية الدليل؟
- حماية البيانات: كيف تحفظ سرية البيانات وأمنها عند انتقالها بين الدول؟
- التفاوت المؤسسي: امتلاك معاهدة لا يساوي امتلاك قدرة فنية وقانونية على تنفيذها.

ومن ثم فإن تقييم بودابست بالنسبة للسودان ينبغي أن يوازن بين فعالية التحقيق وحماية الحقوق والسيادة، دون افتراض نتيجة مسبقة بشأن الانضمام.

10. من الدليل الإلكتروني إلى تتبع عائدات الجريمة

في جرائم الاحتيال الإلكتروني ذات العائد المالي يوجد مساران يجب أن يتحركا بصورة متوازية: مسار الدليل الرقمي ومسار المال. تساعد بودابست في الجانب الأول، بينما تدخل في الجانب الثاني القوانين الوطنية واتفاقيات وآليات مكافحة غسل الأموال واسترداد الأصول.

Budapest: الدليل الإلكتروني والتعاون السيبراني | Warsaw CETS 198: غسل الأموال والبحث والضبط والمصادرة واسترداد العائدات

اتفاقية وارسو CETS No.198 متخصصة في غسل الأموال والبحث والضبط والمصادرة لعائدات الجريمة وتمويل الإرهاب. وفي مايو 2026 اعتمد مجلس أوروبا بروتوكولاً إضافياً لتحديث أدوات استرداد الأصول وتعزيز التعاون الدولي، وحدد 14 أكتوبر 2026 موعداً لفتحه للتوقيع.

iPROCEEDS

iPROCEEDS مشروع مشترك لمجلس أوروبا والاتحاد الأوروبي استهدف تعزيز قدرة السلطات في الدول المشاركة على البحث والضبط والمصادرة لعائدات الجرائم السيبرانية ومنع غسل الأموال على الإنترنت. وهو مشروع عملي وليس اتفاقية أو منصة أنشأتها بودابست.

التتبع ≠ التجميد ≠ المصادرة ≠ الاسترداد.

11. نموذج عملي للتحقيق السيبراني المالي

1. استلام البلاغ وتحديد الواقعة والأضرار.
2. تأمين الأدلة الموجودة لدى المجني عليه وعدم إتلافها.
3. تحديد الحساب أو الرقم أو الرابط أو الجهاز أو المنصة ذات الصلة.
4. تحديد البيانات المعرضة للزوال وطلب حفظها بالطريق القانوني المتاح.
5. تحديد مزود الخدمة والدولة التي توجد فيها البيانات أو الجهة الحائزة لها.
6. تحديد نوع البيانات المطلوبة: معلومات مشترك، بيانات مرور، محتوى، أو بيانات متاحة للعامة.
7. استخدام قناة التعاون القانونية المناسبة للحصول على البيانات.
8. توثيق مصدر الدليل وسلامته وسلسلة حيازته وحجيته.
9. بدء تحقيق مالي موازٍ عند وجود عائد مالي.
10. تحديد الحساب المستفيد وتتبع التحويلات والحسابات الوسيطة والأصول.
11. اتخاذ إجراء تحفظي قانوني عند توافر شروطه لمنع تبديد المال.
12. استخدام التعاون الدولي عند عبور الدليل أو المال الحدود.
13. استكمال إجراءات المصادرة والاسترداد ورد الحقوق وفق القانون المختص.

الجريمة ← الدليل ← الحفظ ← الإفصاح ← التحليل ← تتبع المال ← التجميد ← المصادرة ← الاسترداد

12. النتائج

- بودابست إطار يجمع بين التجريم والإجراءات والتعاون الدولي، وليس مجرد قائمة بجرائم الإنترنت.
- القيمة العملية الكبرى للاتفاقية تظهر عند عبور الدليل الإلكتروني الحدود أو تعرضه للزوال.
- شبكة 24/7 أداة للمساعدة العاجلة وليست سلطة فوق وطنية.
- البروتوكول الثاني يطور التعاون في الأدلة الإلكترونية لكنه لا يمنح وصولاً مفتوحاً إلى بيانات الشركات.
- وجود تقارب في التجريم السوداني لا يكفي وحده لإثبات المواءمة الإجرائية والمؤسسية.
- تتبع عائدات الجريمة وتجميدها ومصادرتها واستردادها مجال متكامل مع بودابست لكنه لا يستمد منظومته كاملة منها.
- فعالية أي نموذج دولي تعتمد على التشريع الوطني والقدرات الفنية والمؤسسية والضمانات الحقوقية.

13. التوصيات

- إجراء مقارنة تشريعية سودانية مادة بمادة تشمل قانون مكافحة جرائم المعلوماتية وقانون الإجراءات الجنائية والتشريعات ذات الصلة.
- دراسة تنظيم الحفظ العاجل للبيانات بصورة واضحة مع الفصل بين الحفظ والإفصاح.
- تطوير تصنيف إجرائي واضح لمعلومات المشترك وبيانات المرور والمحتوى.
- دراسة تطوير نقطة اتصال وطنية متخصصة للتعاون العاجل في الأدلة الإلكترونية.
- إعداد نماذج موحدة للطلبات الدولية تتضمن الحساب، نوع البيانات، الفترة، الأساس القانوني ودرجة الاستعجال.
- تعزيز تدريب أعضاء النيابة والمتحرين والخبراء على الأدلة الرقمية والتعاون الدولي.

• تعزيز التحقيق المالي الموازي في جرائم الاحتيال والجرائم السيبرانية ذات العائد المالي.
• وضع ضمانات واضحة للخصوصية وحماية البيانات وحقوق الغير حسن النية.
• إذا طُرحت مسألة الانضمام مستقبلاً، إجراء دراسة أثر تشريعي ومؤسسي قبل اتخاذ القرار.

14. الخاتمة

أصبحت مكافحة الجريمة السيبرانية مرتبطة بقدرة أجهزة العدالة على التحرك عبر ثلاثة مسارات متزامنة: إثبات الجريمة، المحافظة على الدليل الإلكتروني والحصول عليه بصورة مشروعة، وتعقب العائد المالي عند وجوده.

توفر اتفاقية بودابست نموذجاً دولياً مهماً للتجريم والإجراءات والتعاون في الأدلة الإلكترونية، لكنها لا تلغي القانون الوطني ولا تحل وحدها مسائل استرداد الأصول. وفي المقابل تكملها أطر أخرى مثل اتفاقية وارسو في مجال غسل الأموال والمصادرة واسترداد العائدات.

عندما تعبر الجريمة الحدود، يجب أن يعرف المحقق أين يوجد الدليل، ومن يحوزه، وكيف يحفظه ويحصل عليه، وأين ذهبت عائدات الجريمة، وما الأداة القانونية المناسبة لكل مرحلة.

15. أهم المصطلحات

المعنى المبسط	المصطلح
حفظ البيانات الموجودة بصورة عاجلة لمنع ضياعها أو تغييرها.	Preservation
تقديم البيانات أو الإفصاح عنها وفق الأساس والإجراء القانونيين.	Production / Disclosure
معلومات المشترك المرتبطة بالحساب أو الخدمة وفق التعريف القانوني.	Subscriber Information
بيانات تتعلق بمسار الاتصال وتوقيته ومصدره ووجهته في حدود القانون.	Traffic Data
مضمون الاتصال نفسه مثل الرسالة أو محتوى البريد.	Content Data
البحث والضبط القانوني للبيانات أو الوسائط.	Search and Seizure
تتبع الأموال أو الأصول المرتبطة بالجريمة.	Tracing
منع التصرف في المال مؤقتاً.	Freezing
الحرمان النهائي من المال أو الأصل وفق القرار القانوني المختص.	Confiscation
العملية الأشمل لاسترداد عائدات الجريمة أو التصرف فيها وفق القانون.	Asset Recovery
تحقيق مالي يسير بالتوازي مع التحقيق الجنائي.	Parallel Financial Investigation
المساعدة القانونية المتبادلة بين الدول.	MLA

16. المراجع الرسمية الأساسية

1. Council of Europe - Convention on Cybercrime (ETS No.185)
https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185

2. Council of Europe - Budapest Convention overview
https://www.coe.int/en/web/cybercrime/the-budapest-convention

3. Council of Europe - 24/7 Network
https://www.coe.int/en/web/cybercrime/24/7-network-new

4. Council of Europe - First Additional Protocol
https://www.coe.int/en/web/cybercrime/first-additional-protocol

5. Council of Europe - Second Additional Protocol (CETS No.224)
https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=224

6. Council of Europe - International cooperation
https://www.coe.int/en/web/cybercrime/international-cooperation

7. Council of Europe - Criminal justice authorities and multinational service providers
https://www.coe.int/en/web/cybercrime/criminal-justice-authorities-and-multi-national-service-providers

8. Council of Europe - iPROCEEDS
https://www.coe.int/en/web/cybercrime/iproceeds

9. Council of Europe - Warsaw Convention CETS 198
https://www.coe.int/en/web/cop198

10. Council of Europe - Additional Protocol to Warsaw Convention (adopted 15 May 2026)
https://www.coe.int/en/web/cop198/additional-protocol

ملاحظة ختامية

ينبغي تحديث بيانات عدد الأطراف والتوقيعات والتصديقات وحالة نفاذ البروتوكولات عند استخدام هذه الورقة بعد سبتمبر 2026، لأن هذه البيانات متغيرة بطبيعتها.