Security Policy Papers | أوراق السياسات الأمنية
https://spp.nauss.edu.sa/index.php/spp
الأمم المتحدة المكتب المعني بالمخدرات والجريمة
مركز الخبرة الإقليمي لمكافحة المخدرات والجريمة
Regional Expertise Center for Combating Drugs and Crime (REC-CDC)
ورقة تحليل سياسات أمنية

الذكاء الاصطناعي في مواجهة الترويج الرقمي للمخدرات: تحليل للواقع واتجاهات الابتكار في الدول العربيَّة

Artificial Intelligence in Countering the Digital Promotion of Drugs: An Analysis of the Current Situation and Innovation Trends in Arab Countries

المخرجات الرئيسة

- يمثِّل الترويج الرقمي للمخدرات ظاهرةً إجراميةً متسارعةَ النمو، تستثمر تقنيات الذكاء الاصطناعي وتحليل البيانات الضخمة؛ لاستهداف بعض الفئات، وإدارة شبكات التهريب العابرة للحدود. وتعمل هذه الشبكات كأنظمة متكيفة متجددة؛ مما يُضعف فاعلية أساليب الرصد والمكافحة التقليدية.
- تُعدُّ شبكات تهريب المخدرات نظمًا معقَّدة ومتكيفة؛ مما يعني أن التصدي لها لا يتحقق بالقوة وحدها، بل يستلزم قدرة مكافئة على التكيف والاستجابة، مستندةً إلى المعايير الدولية للوقاية بوصفها مرجعًا علميًّا لبناء منظومات وقائية رقمية فاعلة.
- تقترح الورقة نموذجًا عربيًّا متكاملًا، يعمل على مسارين متوازيين: مسار خفض العرض، ومسار خفض الطلب، عبر توظيف أنظمة الذكاء الاصطناعي كأداة محورية في كليهما.
- أوصت الورقة ببعض الإجراءات المتكاملة، أبرزها: إنشاء منصة عربية للاستشراف الأمني التنبئي،

وإطلاق برامج تدريبية للكوادر الهجينة (أمنية وتقنية ووقائية)، وتأسيس مختبر إقليمي لتطوير الخوارزميات في السياق العربي، وصياغة ميثاق عربي لحماية الحقوق الرقمية في تطبيقات الذكاء الاصطناعي لمكافحة المخدرات.

المستخلص

يشهد الترويج الرقمي للمخدرات والمؤثرات العقليَّة تحولًا نوعيًّا، يعتمد على تقنيات الذكاء الاصطناعي والخوارزميات المتقدمة؛ حيث تستفيد الجماعات

Abstract

Digital promotion of drug and psychoactive substance is undergoing a qualitative transformation driven by artificial intelligence

الإجراميَّة من تحليل البيانات الضخمة، وتوليد المحتوى المخصص عبر أنظمة التزييف العميق، وإدارة شبكات التهريب باستخدام منصات مشفرة وعملات رقمية غير قابلة للتتبع. وفي المقابل، تظلُّ بعض أجهزة المكافحة العربيَّة تعتمد في غالبيتها على أساليب رصد قد لا تستطيع في أكثر الأحيان مجاراة هذا التطور، كما يفتقر كثير منها إلى أطر واضحة لدمج الوقاية الرقمية وحماية الحقوق الأساسية. وتستند هذه الورقة إلى إطار نظري متعدد الأبعاد، يبدأ من الإقرار بأن شبكات المخدرات تعمل كنظم معقَّدة، وأخرى متكيفة؛ مما يستلزم ألا تقتصر إستراتيجيات المكافحة على القوة، بل أن تكون هي الأخرى رشيقة ومرنة وقابلة للتكيف. وتعتمد الورقة على تحليل بيانات دراسة أجرتها جامعة نايف العربيَّة للعلوم الأمنية، شملت عددًا من الدول العربيَّة، وعلى مراجعة منهجية لأدبيات الذكاء الاصطناعي في إنفاذ القانون والاستخبارات التنبئية وحقوق الإنسان الرقمية والمعايير الدولية للوقاية من المخدرات. وتخلص الورقة إلى أن النجاح في مواجهة الترويج الرقمي يقتضي وجود إستراتيجية وطنية وإقليمية، تدمج الابتكار التقني مع الوقاية القائمة على الأدلة واحترام الحقوق الرقمية.

technologies and advanced algorithms. Criminal networks exploit big data analytics, generate customized content through Deepfake systems, and manage trafficking networks using encrypted platforms and untraceable digital currencies. In contrast, most Arab counter-narcotics agencies continue to rely on monitoring methods that often fail to keep pace with this evolution, and many lack clear frameworks for integrating digital prevention and protecting fundamental rights. This paper is grounded in a multi-dimensional theoretical framework, beginning with the recognition that drug networks operate as complex and adaptive systems, which necessitates that counter-strategies not be limited to force alone but must also be agile, flexible, and capable of adaptation. The paper draws on data analysis from a study conducted by Naïf Arab University covering eight Arab countries, as well as a systematic review of the literature on artificial intelligence in law enforcement, predictive intelligence, digital human rights, and international drug prevention standards. The paper concludes that effectively confronting digital promotion of drugs requires national and regional strategies that integrate technological innovation with evidence-based prevention and respect for digital rights.

1. المقدمة

لم يَعُد مسرح جريمة المخدرات بقعةً جغرافيةً محددةً، بل تحوَّل إلى فضاء هجين عابر للحدود، يمزج بين العالمين السيبراني والمادي. فقد انتقلت عمليات الترويج والاتجار من الشوارع والمنافذ الحدودية إلى منصات التواصل الاجتماعي، وتطبيقات المراسلة المشفرة، وأسواق الويب المظلم؛ حيث تُدير الجماعات الإجرامية عملياتها بأقل قدر من المخاطر، وأعلى درجة من السرية (عثمان وآخرون، 2025؛ INTERPOL, 2024b).

وتكشف دراسة ميدانية شملت ثماني دول عربية أن 58% من الشباب العربي على دراية بوجود أسواق إلكترونية للمخدرات، وأن 17% من العينة أقرّوا بتأثرهم بالمحتوى الترويجي، في حين ارتبط التعرض لهذا المحتوى بتجربة التعاطي (عثمان وآخرون، 2025). وتبقى هذه النتائج - رغم محدودية الاستدلال السببي - مؤشرً مهمًّا، يكشف عن ثغرات في منظومة الرقابة الرقمية تستوجب تدخلًا تنظيميًّا عاجلًا.

وفي هذا السياق، تبرز قدرات الذكاء الاصطناعي كأداة ذات حدين؛ إذ توظِّفها الشبكات الإجرامية لتحليل سلوك المستخدمين، وتوليد محتوى ترويجي مخصص (Hu et al., 2023)، في حين تُتيح للجهات المعنية بالمكافحة إمكانات غير مسبوقة في الاستخبارات التنبئية والرصد الآلي والوقاية الرقمية (البابلي، 2023). غير أن هذا التوظيف يطرح إشكاليات قانونية وأخلاقية تتعلق بحماية الخصوصية ومنع التمييز الخوارزمي وضمان المساءلة (Engel et al., 2025؛ Chen, 2023)، وهي إشكاليات لا يمكن إغفالها في أي إطار سياساتي ناضج.

وتنطلق الورقة من تساؤل محوري فحواه: كيف يمكن للدول العربيَّة - في ظل تحديات الرصد الرقمي وصعوبات تغطية المحتوى العربي على منصات التواصل، وغياب التشريعات الموحدة، ومحدودية القدرات المؤسسية في بعض السياقات - أن توظِّف الذكاء الاصطناعي توظيفًا متكاملًا في مواجهة الترويج الرقمي للمخدرات؟

وللإجابة عن هذا التساؤل، تستند الورقة إلى إطار نظري ثلاثي الأبعاد: تُشكّل نظرية التعقيد (Prigogine & Stengers, 1984) بُعده الأول؛ إذ تُثبت أن شبكات التهريب تعمل كنظم متكيفة، تتجاوز المقاربات الأمنيَّة الخطية التقليدية؛ وتُمثّل نظرية النظم المتكيفة (Holland, 1995) بُعده الثاني؛ إذ تؤكد أن فاعلية أي نظام مكافحة تقوم على قدرته على التكيف لا على قوته الثابتة فحسب؛ في حين تُشكِّل المعايير الدولية للوقاية الصادرة عن UNODC وWHO بُعده الثالث، بوصفها مرجعية علمية لبناء منظومات وقائية رقمية قائمة على الأدلة. وعلى هذه الأطر المتكاملة تتأسس التوصيات التنفيذية التي تُختَتم بها الورقة.

2. واقع الترويج الرقمي للمخدرات والمؤثرات العقلية وتحدياته

1.2 مسرح الجريمة الجديد: من المعالم الفيزيقية المحددة إلى الفضاء السيبراني - المادي

شهد مسرح جريمة المخدرات تحولًا بنيويًّا عميقًا؛ إذ لم تَعُد الشبكات الإجرامية مرتبطةً بمواقع جغرافية محددة قابلة للرصد والضبط، بل باتت تعمل في فضاء هجين، يجمع بين العالمين المادي والرقمي. فهذه الشبكات تختفي خلف أسواق الويب المظلم المشفرة، وتُدير عملياتها عبر تطبيقات تلاشي الرسائل، وتُموِّل صفقاتها بعملات رقمية يصعب تعقُّبها (INTERPOL, 2024b) وقد أضافت تقنيات الذكاء الاصطناعي بُعدًا جديدًا لهذا التحول، من خلال توليد هُويات وصور مزيفة لأغراض الترويج، وابتكار آليات تشفير متقدمة تمنع اختراق هذه الشبكات.

وأمام هذا الواقع، لم تَعُد أدوات الرصد والضبط التقليدية كافيةً بصورتها الكلاسيكية. فبينما يوظّف

المجرمون الذكاء الاصطناعي لإخفاء هُوياتهم وتعقيد مساراتهم، بات لزامًا على جهات المكافحة استثمار التقنيات ذاتها؛ للكشف عن الأنماط الخفية وتحليل الشبكات. غير أن هذا التحول لا يتحقق دون بنية تحتية متطورة، وكوادر مدربة على الجمع بين الكفاءتين الأمنيَّة والتقنية، وأطر قانونية واضحة تُنظِّم توظيف هذه التقنيات وتضمن المساءلة (الغسية، 2022).

2.2 قصور الاستجابات التقليدية

لا يزال عدد من الأجهزة الأمنيَّة العربيَّة يراهن على الرصد اليدوي للمحتوى الرقمي، وهو أسلوب ثبتت محدوديته أمام الحجم الهائل من البيانات التي تنتجها منصات التواصل الاجتماعي يوميًّا. وقد كشفت الدراسة الميدانية عن أربع نقاط ضعف جوهرية تُقيِّد فاعلية المنظومة الأمنيَّة العربيَّة في هذا الموضوع كما يأتي (عثمان وآخرون، 2025):

- **محدودية التعاون الأمني العربي:** تتضافر في إنتاج هذه المحدودية عوامل بنيوية متشابكة، أبرزها: تباين أولويات الأمن الوطني بين الدول، وغياب بنية تحتية رقميَّة مشتركة، تُتيح التبادل الفوري للمعلومات، وافتقار المنظومة القانونية الإقليمية إلى أطر موحدة لتبادل الأدلة الرقمية، فضلًا عن شُح الكوادر التقنية المشتركة القادرة على تشغيل أنظمة الذكاء الاصطناعي الأمنيَّة وتطويرها.
- **ضعف الإشراف على المحتوى العربي:** كشفت الدراسة عن إخفاق واضح لمنصات ميتا وتيك توك وسناب شات في حجب المحتوى الترويجي الصريح باللغة العربيَّة؛ إذ أسفرت عمليات بحث بسيطة عن مصطلحات من قبيل «بيع الكبتاجون» أو «حشيش للبيع» عن نتائج مباشرة دون الحاجة إلى أي لغة مشفرة. وهذا القصور يعكس غياب سياسة إقليمية ضاغطة، تُلزم المنصات بمعالجة المحتوى العربي بالمستوى ذاته المعمول به في اللغات الأخرى.
- **فصل الهُويَّة الرقمية عن الهُويَّة المادية:** تُشير تصريحات رسمية إلى وجود أكثر من 14 مليون حساب وهمي في دولة عربية واحدة؛ مما يُصعِّب ربط هذه الحسابات بأشخاص حقيقيين في غياب قواعد بيانات بيو مترية موحدة. والأكثر دلالةً أن 58% من مستجيبي الدراسة أبدوا وعيًا بهذه الثغرة؛ مما يكشف أن الفجوة ليست في الوعي العام، بل في الإرادة التنظيمية والقدرة المؤسسية.
- **ارتفاع التعرض للمحتوى الترويجي وأثره في الطلب:** أفادت نسبة معتبرة من عينة الدراسة أن التعرض للمحتوى الترويجي كان دافعًا للتفكير في التعاطي، أو تجربته، وهو ما يُرسِّخ الحاجة إلى مقاربة مزدوجة، تجمع بين ضبط العرض الرقمي وتحصين جانب الطلب.

3.2 التقنيات المتاحة: الفرص والتحديات

تُظهر الأدبيات المعاصرة نضجًا ملحوظًا في أربعة مسارات تكنولوجية قابلة للتوظيف في السياق العربي، وإن كان لكل مسار اشتراطاته وتحدياته الخاصة:

1. **الخوارزميات التنبئية وتحليل الشبكات (خفض العرض):** تُوظِّف هذه الخوارزميات تقنيات التصنيف والتجميع والتنبؤ لتحليل البيانات الضخمة المرتبطة بالأنشطة الإجرامية، وتحديد أنماط التهريب، وتوقع مساراته المحتملة (البابلي،

2023). ويمكن توظيفها في السياق العربي لتحليل حركة الشحن والتحويلات المالية عبر العملات المشفرة، ورصد تحولات السوق نحو مواد جديدة بيد أن اشتراط الفاعلية يقتضي اقتران تطبيقها بآليات للمراجعة البشرية والشفافية الخوارزمية درءًا لمخاطر التمييز .(Chen, 2023)

2. **الأنظمة البيومترية المتقدمة (خفض العرض):** تشمل التعرف على الوجه والقزحية والصوت وأنماط المشية، وقد أتاحت منصة الإنتربول البيومترية تبادلها بين 196 دولة (INTERPOL, 2024a) غير أن هذه الأنظمة تُثير مخاوف جدية تتعلق بالخصوصية والمراقبة الجماعية؛ مما يستوجب تقييدها بضوابط تشريعية واضحة، تشمل الإذن القضائي المسبق، وتحديد حالات الاستخدام وفترات الاحتفاظ بالبيانات، وضمان حق الطعن في القرارات الخوارزمية (Clanx, 2024).

3. **تحليل سلاسل الكتل (خفض العرض):** طوّرت FATF والإنتربول أدوات فاعلة لتتبع معاملات العملات المشفرة المشبوهة، أسهمت في تفكيك شبكات تمويل إجرامية. ويبقى التحدي الرئيس في العملات التي تُركِّز على الخصوصية، مما يستدعي تشريعات تُحدد صلاحيات الوصول إلى البيانات المالية الرقمية مع ضمانات قضائية كافية.

4. **أنظمة كشف المحتوى الضار والوقاية الرقمية (خفض الطلب):** يمكن توظيف خوارزميات معالجة اللغة الطبيعية والتعلم العميق لرصد المحتوى الترويجي وإزالته، وتوجيه المستخدمين نحو بدائل توعوية (Klonick, 2020). كما تُتيح روبوتات الدردشة المدعومة بالذكاء الاصطناعي تقديم الدعم النفسي والإرشاد الوقائي للشباب المعرَّضين للخطر مع صون سرية بياناتهم (UNODC & WHO, 2018). ويُشكِّل هذا المسار الحلقة الأكثر إلحاحًا في السياق العربي؛ نظرًا للفجوة الواسعة الراهنة في تغطية المحتوى العربي.

يلخص جدول 1 المسارات التقنية الأربعة.

جدول 1
المسارات التقنية الأربعة

المسار	التطبيق	التحديات	الضمانات المطلوبة
الخوارزميات التنبئية (خفض العرض)	تحليل أنماط التهريب، توقع العمليات، تعقب العملات المشفرة.	تمييز خوارزمي، تحيزات في البيانات.	مراجعة بشرية، شفافية خوارزمية.
الأنظمة البيومترية (خفض العرض)	تعرّف على الوجه، قزحية، صوت، بصمات.	خصوصية، مراقبة جماعية.	إذن قضائي، خصوصية تفاضلية، حق الاعتراض.
تحليل سلاسل الكتل (خفض العرض)	تتبع معاملات العملات المشفرة المشبوهة.	عملات تركز على الخصوصية، تعارض مع الخصوصية المالية.	تشريعات تحدد صلاحيات الوصول بضمانات قضائية.
كشف المحتوى الضار والوقاية الرقمية (خفض الطلب)	NLP، تعلم عميق، روبوتات دردشة وقائية.	سرية البيانات، دقة التصنيف.	عدم تخزين بيانات المستخدمين، شفافية.

الجدول من إعداد الباحثين

3. توظيف الذكاء الاصطناعي في المواجهة

1.3 نقلة نوعية في مكافحة الاتجار بالمخدرات

لقد أضحت قدرات الذكاء الاصطناعي على تحليل البيانات الضخمة، وتتبع الأنشطة الإجرامية في الفضاء الرقمي تحولًا جوهريًّا في منظومة إنفاذ القانون (INTERPOL, 2024b). فبعد أن أتاحت شبكات التشفير كـ«تور» للجماعات الإجرامية العمل بعيدًا عن الرقابة التقليدية، جاءت تقنيات الذكاء الاصطناعي لتُعيد التوازن؛ إذ تكشف الأنماط السلوكية التي تنتج عن عمليات الإخفاء ذاتها، وتُمكِّن المحققين من مسح الأسواق غير المشروعة وفق معايير بحث متقدمة أثبتت

فاعليتها في عزل أنشطة الاتجار بالمخدرات والكشف عن شبكاتها (Hu et al., 2023).

غير أن تحقيق هذه النقلة النوعية يظلُّ رهينًا بتوافر ثلاثة شروط مؤسسية متلازمة: بنية تحتية بيانية مشتركة، وكوادر هجينة تجمع بين الكفاءتين الأمنيَّة والتقنية، وأطر قانونية تُجيز توظيف هذه التقنيات وتُحدد ضوابطها.

2.3 توظيف الذكاء الاصطناعي في العلاج والتأهيل

لا يقتصر دور الذكاء الاصطناعي على الجانب الأمني لخفض العرض، بل يمتد إلى مسار خفض الطلب عبر تطبيقات علاجية ووقائية واعدة. فمنصات الرعاية الصحية عن بُعد وروبوتات الدردشة وخدمات الاستشارات الافتراضية المدعومة بالذكاء الاصطناعي باتت تُتيح خيارات دعم نفسي وإرشاد علاجي للأفراد المعرّضين لخطر التعاطي، أو الواقعين في فخ الإدمان، بما يتجاوز حواجز الوصول الجغرافية والاجتماعية (UNODC & WHO, 2018)، كما تبرز إمكانات الذكاء الاصطناعي في التنبؤ بمخاطر الانتكاس ومنعه لدى الأفراد في مرحلة التعافي؛ مما يُعزز استدامة نتائج برامج التأهيل (Hu et al., 2023).

وفي السياق العربي تحديدًا، يُمثِّل هذا المسار فرصة سياساتية لم تُستثمر بعد؛ إذ يمكن لهذه الأدوات أن تسد الفجوة بين الطلب على خدمات الدعم النفسي ومحدودية العرض المؤسسي، شريطة أن تُبنى وفق معايير تحمي خصوصية المستخدمين، وتراعي الخصوصية الثقافية للمجتمعات العربيَّة.

4. تحليل الخيارات الإستراتيجية والدروس المستفادة

1.4 تجارب دولية وممارسات فضلى

تكشف التجارب الدولية عن مسارين متكاملين في توظيف الذكاء الاصطناعي لمكافحة الاتجار بالمخدرات: مسار تعزيز قدرات إنفاذ القانون، ومسار تطوير التعاون المعلوماتي الدولي.

على صعيد إنفاذ القانون، تبرز عملية I-RAID/ Lionfish Hurricane التي قادها الإنتربول نموذجًا متقدمًا لدمج تحليلات البيانات الضخمة والذكاء الاصطناعي والتعاون الدولي؛ إذ أسفرت عن ضبط 615 طنًا من المخدرات واعتقال 31 شخصًا عبر تحليل أنماط التهريب وتتبع التدفقات المالية (INTERPOL, 2024b)، وعلى المنوال ذاته، يمتلك مركز الجرائم الإلكترونية الأوروبي (يوروبول) قدرات متطورة في تعقب العملات المشفرة، وتحليل شبكات الاتصال الإجرامية على الويب المظلم.

وعلى صعيد التعاون المعلوماتي، أنشأ الإنتربول قاعدتَي بيانات SLTD و FIELDSلتبادل المعلومات الفوري حول وثائق السفر المشبوهة بين 196 دولة (INTERPOL, 2024a)، في حين يُمثّل برنامج (SMART) التابع لـ UNODC نموذجًا رائدًا في الإنذار المبكر بالمؤثرات العقلية المستجِدة وتحليل مخاطرها (عثمان وآخرون، 2025). أما على مستوى المنصات الرقمية، فقد أثبتت تجربة فيسبوك في اكتشاف المحتوى الضار وإزالته آليًّا قبل الإبلاغ عنه إمكانية التطبيق الواسع النطاق لهذه الأنظمة (Klonick,

2020)، وإن كانت لا تزال تُسجِّل قصورًا ملحوظًا في معالجة المحتوى العربي تحديدًا.

2.4 تحليل الخيارات الإستراتيجية المتاحة

الخيار الأول: الرصد اليدوي والضبطيات الكلاسيكية: يُمثِّل هذا الخيار مسارًا منخفض التكلفة، يتفادى تعقيدات الاستثمار التقني والإشكاليات القانونية المرتبطة بحماية البيانات. غير أن عيوبه جوهرية؛ فهو عاجز عن مواكبة التطور المتسارع لأساليب الشبكات الإجرامية، ويترك المواطنين عرضةً للمخاطر الرقمية دون حماية استباقية فاعلة.

الخيار الثاني: التبني المنفرد لأدوات الذكاء الاصطناعي دون تكامل إقليمي: يقوم هذا الخيار على اقتناء أنظمة جاهزة لأغراض محددة كمراقبة المنافذ الحدودية، أو رصد الويب المظلم، دون ربطها بمنظومة إقليمية أو إطار قانوني موحد. وهو يُحسِّن الأداء نسبيًّا في نقاط بعينها، لكنه يظل قاصرًا عن مواجهة شبكات التهريب العابرة للحدود التي تستثمر تحديدًا الفجوات بين الأنظمة الوطنية المتفرقة.

الخيار الثالث: النهج المتكامل مع ضمانات حقوقية (الخيار الموصى به) يقوم هذا الخيار على إنشاء منظومة عربية متكاملة تجمع الخوارزميات التنبئية والأنظمة البيومترية وأدوات الوقاية الرقمية (Chen, 2023; Clanx, 2024)، مع اعتماد مبادئ الخصوصية التفاضلية والشفافية الخوارزمية والمراجعة البشرية الإلزامية ضمانةً للحقوق الأساسية. ويتميز بقدرته على الرصد الشامل في الوقت الفعلي، ومعالجة جانبَي العرض والطلب في آنٍ معًا، وبناء الثقة المجتمعية في المنظومة الأمنيَّة. ويستلزم تطبيقه استثمارات مالية وبشرية معتبرة، وإصلاحات تشريعية ومؤسسية منسَّقة على المستوى الإقليمي.

5. نحو نموذج مرن متعدد الأبعاد لمواجهة الترويج الرقمي بالذكاء الاصطناعي في الدول العربيَّة

يقوم النموذج المقترح على أربعة أبعاد متكاملة، تعمل معًا على مسارَي خفض العرض وخفض الطلب:

البعد الأول: الاستشراف الأمني التنبئي (خفض العرض)

يتمثل هذا البعد في إنشاء منصة عربية للاستشراف الأمني التنبئي، تعتمد على خوارزميات التعلم الآلي وتحليل الشبكات والتحليل المكاني (GIS)، وتعمل على ثلاثة محاور:

- تحليل أنماط التهريب وتوقع المسارات الأكثر عرضة للاختراق، استنادًا إلى البيانات التاريخية والمتغيرات الآنية.
- تعقب تدفقات العملات المشفرة، بالتعاون مع وحدات التحليل المالي الوطنية والدولية.
- التنبؤ بظهور مواد مخدرة جديدة، من خلال رصد المنشورات العلمية، وسجلات الضبط، واتجاهات البحث الرقمي، بما يتماشى مع نموذج الإنذار المبكر لبرنامج SMART.

وتُطبَّق على هذه المنصة مبادئ الخصوصية التفاضلية التي تُتيح تحليل البيانات الضخمة دون

الكشف عن هُويات غير المتورطين، فيما تُعهد مراجعة المخرجات الخوارزمية إلى لجنة مستقلة تضم خبراء أمنيين وقانونيين وحقوقيين.

البعد الثاني: الدمج بين الأنظمة البيومترية والهُوية الرقمية (خفض العرض مع ضمانات)

يتأسس هذا البعد على قاعدة بيانات بيومترية عربية موحدة، تشمل صور الوجه وبصمات الأصابع وقياسات القزحية والتوقيع الصوتي، مع إتاحة الوصول الآني لمنافذ الدخول الحدودية على غرار منصة الإنتربول البيومترية. ويُرافق إنشاء هذه القاعدة اعتماد مدونة السلوك العربيَّة للبيانات البيومترية، التي تُحدد حالات الاستخدام المسموحة، وفترات الاحتفاظ بالبيانات، وحق الأفراد في الاعتراض على النتائج الخوارزمية والتماس مراجعة بشرية، وعقوبات التجاوزات.

والتأكيد هنا جوهري: ينبغي أن تبقى المخرجات الخوارزمية قرائن استرشادية لا أحكامًا نهائية؛ إذ أثبتت التجارب الدولية أن الاعتماد الكامل على الخوارزميات في التصنيف الجنائي يُفضي إلى تحيزات خطيرة تمس حقوق الأفراد.

البعد الثالث: أنظمة كشف المحتوى الضار والوقاية الرقمية (خفض الطلب)

يقوم هذا البعد على ركيزتين متكاملتين:

الركيزة الأولى: المرصد الإلكتروني للترويج الضار: يستخدم خوارزميات معالجة اللغة الطبيعية والتعلم العميق؛ لتحليل منشورات التواصل الاجتماعي وأسواق الويب المظلم؛ بهدف كشف اللغة المشفرة والحسابات الترويجية، وتحديد المؤثرين في شبكات الاتجار، مع الإبلاغ الفوري للمنصات لإزالة المحتوى والاحتفاظ بسجلات الأدلة الرقمية.

الركيزة الثانية: منصة الوقاية الرقمية التفاعلية: تستهدف خفض الطلب عبر أربعة مسارات: توفير محتوى توعوي بديل يظهر تلقائيًّا للمستخدمين الذين يبحثون عن كلمات مفتاحية مرتبطة بالمخدرات؛ وتشغيل روبوتات دردشة مدعومة بالذكاء الاصطناعي؛ لتقديم الدعم النفسي للشباب مع ضمان السرية التامة؛ وإنشاء منصات لتبادل تجارب المتعافين بديلًا عن منتديات الترويج؛ ودمج برامج المهارات الحياتية في منصات التعلم الإلكتروني وفق المعايير الدولية للوقاية (UNODC & WHO, 2018).

البعد الرابع: بناء القدرات الهجينة وإطار الحوكمة الأخلاقية

لا يقوم هذا النموذج دون استثمار حقيقي في تكوين كوادر وطنية «هجينة» تجمع ثلاث مجموعات من المهارات: المهارات الأمنيَّة التقليدية (التحري الميداني وإدارة المصادر السرية)؛ والمهارات الرقمية المتقدمة (تحليل الخوارزميات واستخبارات المصادر المفتوحة OSINT وتحليل سلاسل الكتل)؛ والمهارات الوقائية والحقوقية (المعايير الدولية للوقاية ومبادئ الخصوصية التفاضلية وحقوق الإنسان الرقمية).

ويُقترح في هذا الإطار برنامج تدريبي إقليمي متقدم بالتعاون مع UNODC والإنتربول واليوروبول،

يتكون من ثلاث وحدات متدرجة، تمتد نحو سبعة أسابيع. ويُستكمل هذا البناء المؤسسي بإنشاء مختبر ابتكار عربي للخوارزميات الأمنيَّة والوقائية (AI4SEC-Lab) لتطوير أدوات عربية مخصصة واختبارها وتقييم أثرها على الحقوق الرقمية قبل نشرها، بالشراكة مع الجامعات ومراكز البحوث وهيئات المجتمع المدني.

يبين جدول 2 الفروق بين مساري خفض العرض وخفض الطلب.

جدول 2
المقارنة بين مساري خفض العرض وخفض الطلب

المسار	الأدوات والتقنيات	المؤسسات المعنية	آليات الحوكمة	مؤشرات الأداء
خفض العرض	خوارزميات تنبئية، تحليل شبكات، تتبع عملات مشفرة، أنظمة بيومترية.	إدارات مكافحة المخدرات، الجمارك، الإنتربول، وحدات التحليل المالي.	خصوصية تفاضلية، إذن قضائي سابق، مراجعة بشرية إلزامية.	نسبة كشف الشحنات، وقت الاستجابة، دقة التطابق.
خفض الطلب	كشف المحتوى الضار (NLP)، روبوتات دردشة وقائية، منصات توعوية تفاعلية.	وزارات الصحة، التعليم، حماية الطفل، منصات التواصل الاجتماعي.	سرية البيانات، عدم تخزين هويات المستخدمين، شفافية الخوارزميات.	نسبة انخفاض التعرض للمحتوى، عدد المستفيدين من البدائل التوعوية.

الجدول من إعداد الباحثين

6. التوصيات: خريطة طريق مرحلية مع مؤشرات أداء لتطوير المسار

تم بناء التوصيات التالية، بالاعتماد على منهجية الاستشراف الإستراتيجية، وبناء السيناريوهات؛ وذلك لضمان تقديم رؤية عملية قابلة للتطبيق، تلبي احتياجات الجهات المعنية، وتدعم عملية اتخاذ القرار في سياق متغير ومعقَّد كالترويج الرقمي للمخدرات. وقد أسهم هذا النهج في استكشاف مسارات مستقبلية متعددة وتقدير تداعياتها المحتملة؛ مما يعزز من واقعية المقترحات وإمكانية تنفيذها. وفي هذا الإطار، تجدر الإشارة إلى أن التقديرات المرتبطة بالتكلفة المالية تم تقديمها في صورة سيناريوهات افتراضية إرشادية، وليست إلزامية؛ إذ تظلُّ قابلة للتعديل بالزيادة، أو النقصان وفقًا لخصائص السياق المؤسسي والتشغيلي الذي سيتم فيه تطبيق التوصيات، وما يرتبط به من متغيرات تقنية وتنظيمية وموارد متاحة، علاوة على ذلك فإن الجهات المقترحة للأخذ بهذه التوصيات وتنفيذها قد تختلف من دولة إلى أخرى، حسب طبيعة الدور والمهام المنوطين بهذه الجهات.

1.6 توصيات المرحلة الأولى (قصيرة المدى)

التوصية الأولى: إنشاء آلية عربية متكاملة لتجاوز محدودية التعاون الأمني الرقمي

المحتوى: تجاوزًا للمعوقات التاريخية التي حدَّت من فاعلية التعاون الأمني العربي في مجال مكافحة الترويج الرقمي للمخدرات، يُقترح اعتماد حزمة متكاملة من الآليات، تشمل:

- إنشاء مجلس تعاون أمني رقمي عربي تحت مظلة جامعة نايف العربيَّة للعلوم الأمنيَّة، يتولى تنسيق الجهود، ووضع المعايير الفنية المشتركة.
- اعتماد بروتوكول عربي لتبادل الأدلة الرقمية مع ضمانات سيادية واضحة، على غرار نموذج اتفاقية بودابست المعدلة بما يتوافق مع السياق العربي.
- تفعيل منصة تجريبية في ثلاث دول كمرحلة أولى، على أن يُتاح التوسع التدريجي لباقي الدول العربيَّة بناءً على نتائج التقييم.
- توفير حوافز أمنية ومالية للدول المشاركة، تشمل الدعم التقني، وبرامج التدريب المتخصص، وتحديث الأنظمة الوطنية.
- إشراك الإنتربول واليوروبول كجهات ضامنة لحيادية المعلومات وسلامة التبادل، مع احترام الخصوصية والسرية.

الجهة المسؤولة: الأمانة العامة لمجلس وزراء الداخلية العرب، بالتنسيق مع جامعة نايف العربيَّة للعلوم الأمنيَّة، والإنتربول، واليوروبول.

تقدير التكلفة: 600-900 ألف دولار (تشمل ورش عمل، وتطوير بروتوكول، وبناء المنصة التجريبية، وحوافز أولية).

مؤشرات القياس: إطلاق المجلس والبروتوكول خلال 12 شهرًا؛ تشغيل المنصة التجريبية بثلاث دول بنهاية العام الأول؛ توقيع خمس دول عربية على الأقل على البروتوكول؛ إصدار تقرير تقييم سنوي حول جودة التبادل وزمن الاستجابة؛ تحقيق تحسن بنسبة 50% في سرعة تبادل الأدلة الرقمية مقارنةً بفترة ما قبل الآليات.

التوصية الثانية: إنشاء منصة عربية للاستشراف الأمني التنبئي

المحتوى: منصة إقليمية، تعتمد على خوارزميات التعلم الآلي وتحليل الشبكات والتحليل المكاني لتحليل أنماط التهريب وتوقع العمليات، وتعقب العملات المشفرة. تُطبق المنصة مبادئ الخصوصية التفاضلية، وتُعهد مراجعة مخرجاتها إلى لجنة مستقلة تضم خبراء أمنيين وقانونيين وحقوقيين.

الجهة المسؤولة: الأمانة العامة لمجلس وزراء الداخلية العرب، بالتعاون مع جامعة نايف العربيَّة للعلوم الأمنيَّة والإنتربول، ومكتب الأمم المتحدة المعني بالمخدرات والجريمة.

تقدير التكلفة: 1.5 مليون دولار.

مؤشرات القياس: إطلاق منصة تجريبية بنهاية العام؛ تدريب 50 محللًا من خمس دول؛ إصدار تقارير شهرية؛ إجراء تقييمين أخلاقيين مستقلين؛ تحقيق دقة مطابقة لا تقل عن 85% للوجوه في ظروف الإضاءة المختلفة.

التوصية الثالثة: إطلاق مشروع تدريبي تجريبي للكوادر الهجينة في ثلاث دول

المحتوى: دورة تدريبية مكثفة (سبعة أسابيع) تجمع بين المهارات الأمنيَّة والرقمية والوقائية والحقوقية، مع إدماج المعايير الدولية للوقاية ومبادئ الخصوصية التفاضلية والشفافية الخوارزمية.

الجهة المسؤولة: جامعة نايف العربية للعلوم الأمنيَّة بالتعاون مع مكتب الأمم المتحدة المعني بالمخدرات والجريمة والإنتربول واليوروبول ومنظمات حقوق الإنسان الرقمية.

تقدير التكلفة: 400 ألف دولار.

مؤشرات القياس: تخريج 90 ضابطًا هجينًا؛ تنفيذ ست عمليات تجريبية؛ إصدار تقرير تقييم مستقل؛ اجتياز 90% من الخريجين اختبار محاكاة عملية هجينة؛ إظهار تحسن بنسبة 40% في وقت الاستجابة مقارنةً بالضباط التقليديين.

2.6 توصيات المرحلة الثانية (المدى المتوسط)

التوصية الرابعة: صياغة ميثاق عربي لحماية الحقوق الرقمية في تطبيقات الذكاء الاصطناعي لمكافحة المخدرات

المحتوى: صياغة ميثاق عربي نموذجي يحدد شروط استخدام البيانات البيومترية والخوارزميات التنبئية في التحقيقات الجنائية، ويُلزم بآليات الخصوصية التفاضلية والمراجعة البشرية الإلزامية والشفافية الخوارزمية، ويؤسس لهيئة مستقلة لمراجعة الشكاوى المتعلقة بالقرارات الخوارزمية. ويُستند في صياغته إلى المبادئ التوجيهية الأوروبية والممارسات الكندية.

الجهة المسؤولة: الأمانة العامة لمجلس وزراء العدل العرب بالتعاون مع خبراء من مكتب الأمم المتحدة المعني بالجريمة والمخدرات والإنتربول ومنظمات حقوق الإنسان الرقمية.

تقدير التكلفة: 300 ألف دولار، تشمل الصياغة والمشاورات والاعتماد.

مؤشرات القياس: إقرار الميثاق في غضون 18 شهرًا؛ اعتماد ثلاث دول عربية على الأقل له أو تعديل تشريعاتها وفقًا له؛ إنشاء هيئة وطنية لمراجعة الشكاوى الخوارزمية في دولة رائدة؛ تسجيل عدد الشكاوى المقدمة ونسبة الحل خلال 30 يومًا.

التوصية الخامسة: إقامة شراكات منظمة مع شركات التكنولوجيا ومنصات التواصل الاجتماعي

المحتوى: توقيع اتفاقيات تعاون محددة المدة (ثلاث سنوات قابلة للتجديد) مع ميتا، وتيك توك، وتليجرام، وسناب شات، تتضمن آليات للإبلاغ السريع عن المحتوى الترويجي (مدة قصوى 24 ساعة للاستجابة)، ووصول مشروط (بإذن قضائي) إلى بيانات الحسابات المشبوهة، وتطوير خوارزميات مشتركة لكشف المحتوى باللغة العربيَّة مع التركيز على اللهجات المختلفة.

الجهة المسؤولة: الأمانة العامة لمجلس وزراء الداخلية العرب بالتنسيق مع الهيئات الوطنية لتنظيم الاتصالات وهيئات حماية البيانات الوطنية.

تقدير التكلفة: 500 ألف دولار، تشمل تكاليف التفاوض، والتنفيذ التقني، والمتابعة.

مؤشرات القياس: توقيع اتفاقيات مع ثلاث شركات كبرى على الأقل؛ رفع نسبة الإزالة إلى 80% من المحتوى المبلغ عنه خلال 24 ساعة؛ عدد القضايا المحالة إلى جهات التحقيق بناءً على أدلة رقمية.

3.6. توصيات المرحلة الثالثة (طويلة المدى)

التوصية السادسة: إنشاء مختبر الابتكار العربي للخوارزميات الأمنيَّة والوقائية ونظام رصد الحقوق الرقمية

المحتوى: مختبر إقليمي لتطوير أدوات خوارزمية مخصصة للسياق العربي (كشف Deepfake، تحليل اللغة المشفرة، تحليل صور الأقمار الاصطناعية، نماذج تنبئية)، ونظام رصد للحقوق الرقمية.

الجهة المسؤولة: جامعة نايف العربيَّة للعلوم الأمنيَّة بالتعاون مع مراكز أبحاث أكاديمية عربية ومنظمات حقوق الإنسان الرقمية الدولية.

تقدير التكلفة: 2.5 مليون دولار، تشمل تكاليف التأسيس والتشغيل لمدة ثلاث سنوات.

مؤشرات القياس: تأسيس المختبر ونظام الرصد بحلول نهاية السنة الثالثة؛ تطوير أداتين تجريبيتين ناجحتين مع تقارير تقييم أخلاقي مصاحبة؛ نشر ستة بحوث علمية في مجلات محكمة (منها اثنان على الأقل في مجال أخلاقيات الخوارزميات الأمنيَّة)؛ عقد مؤتمرين إقليميين سنويين حول الابتكار في مكافحة الترويج الرقمي للمخدرات.

المراجع

المراجع العربيَّة

البابلي، عمار ياسر. (2023). الذكاء الاصطناعي في مواجهة الشائعات وجرائم تمويل الإرهاب في البيئة السيبرانية. القاهرة: المنظمة العربيَّة للتنمية الإدارية.

الغسية، حمدان. (2022). خارطة الطريق لاستشراف المستقبل في العمل الأمني. دبي: مركز استشراف المستقبل.

عثمان، عمرو؛ شرف، عبد السلام؛ كيم، كيونغون؛ معلوف، وديع. (2025). الترويج الإلكتروني للمواد المخدرة والمؤثرة على الحالة النفسية: الواقع وآليات المواجهة. الرياض: جامعة نايف العربيَّة للعلوم الأمنيَّة.

المراجع الأجنبية

Chen, Z. (2023). Ethics and discrimination in artificial intelligence-enabled recruitment practices. Humanities and Social Sciences Communications, 10, Article 567.

Clanx. (2024,). Differential privacy in AI: Examples of differential privacy in AI.

Engels, C., Linhardt, L., & Schubert, M. (2025). Code is law: How COMPAS affects the way the judiciary handles the risk of recidivism. Artificial Intelligence and Law, 33(2), 383-404.

Holland, J. H. (1995). Hidden order: How adaptation builds complexity. Addison-Wesley.

Hu, C., Zhang, M., Liu, Q., & Wang, X. (2023). Fine-grained classification of drug trafficking based on Instagram hashtags. Decision Support Systems, 165, 113896.

to adjudicate online free expression. The Yale Law Journal, 2418-2486.

Prigogine, I., & Stengers, I. (1984). Order out of chaos: Man's new dialogue with nature. Bantam Books.

UNODC, & WHO. (2018). International standards on drug use prevention (2nd Ed.). UNODC.

INTERPOL. (2024a). FIELDS and SLTD databases annual report 2023. INTERPOL General Secretariat.

INTERPOL. (2024b). Operation Lionfish Hurricane: Results and lessons learned. INTERPOL General Secretariat.

Klonick, K. (2020). The Facebook Oversight Board: Creating an independent institution

July 2026

يوليو 2026

Regional Expertise Centre for Combating Drugs and Crime

مركز الخبرة الإقليمي لمكافحة المُخدِّرات والجريمة

Naif Arab University for Security Sciences
Riyadh, Saudi Arabia

جامعة نايف العربية للعلوم الأمنية
الرياض، المملكة العربية السعودية

Keyword

artificial intelligence, digital drug promotion, supply reduction, demand reduction, predictive algorithms, biometric systems, digital rights

الكلمات المفتاحية

الذكاء الاصطناعي، الترويج الرقمي للمخدرات، خفض العرض، خفض الطلب، الخوارزميات التنبئية، الأنظمة البيومترية، الحقوق الرقمية

Production and hosting by NAUSS

Email: recdc@nauss.edu.sa
doi: 10.26735/NZZP4155