Article

JOURNAL OF UNIVERSITY OF BABYLON
For Pure and Applied Sciences (JUBPAS)
Special Issue 1: The First Babylon Conference on Countering Extremism and Terrorist Violence in Light of Global Political Shifts

Vol, 33; S.1 | 2025

Identifying The Nature of Security Threats Associated with Terrorist Digital Content and Its Impact on Cyber Genocide

Hawraa Adel Nori[1], Mithal Hadi Jebor[2], Israa Adel Nori[3]

[1] Computer Center, University of Babylon, hawraa.adel@uobabylon.edu.iq ,Babylon, Iraq
[2] Computer Center, University of Babylon, mithalhadi@uobabylon.edu.iq ,Babylon, Iraq
[3] College of Engineering, University of Babylon, eng.asraa.adel@uobabylon.edu.iq ,Babylon, Iraq

تحديد طبيعة التهديدات الامنية المرافقة للمحتوى الرقمي الارهابي وتاثيره على الإبادة المعلوماتية

حوراء عادل نوري[1]، مثال هادي جبر[2]، اسراء عادل نوري[3]

1 مركز الحاسبة الالكترونية ، جامعة بابل ، hawraa.adel@uobabylon.edu.iq ، بابل، العراق
2 مركز الحاسبة الالكترونية ، جامعة بابل ، mithalhadi@uobabylon.edu.iq ، بابل، العراق
3 كلية الهندسة ، جامعة بابل ، eng.asraa.adel@uobabylon.edu.iq ، بابل، العراق

Received: 18/8/2025 **Published:** 28/8/2025

ABSTRACT

This study examines the growing conflict between the need to combat online terrorist content and the fundamental principles of expression freedom and knowledge preservation. While the current model of content moderation responding to legitimate security threats, it poses a significant and under-researched risk: information genocide—the systematic devaluation, silencing, and annihilation of knowledge systems through digital erasure.

By analyzing the technical architecture of algorithmic moderation and the geopolitical forces, that shaping content policies and legal frameworks governing online discourse. The study highlights the crisis of balancing digital security with the protection of fundamental rights. Strict censorship measures can have negative counterproductive effects, such as inadvertently destroying vital evidence of human rights violations, silencing legitimate counter narratives, and eroding the digital cultural record.

The study analyzes the cyber risks associated with terrorist content, critiques the opacity and biases of automated systems, and conceptualizes digital epistemic genocide as a significant harm. It concludes by proposing a multi-stakeholder framework for rights-preserving content governance and calling for a paradigm shift from blunt censorship to careful regulation that balances proactive removal with robust archival preservation.

Keywords: cyber threats, risks, terrorist content, cyber genocide, censorship, digital archives

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

Article
JOURNAL OF UNIVERSITY OF BABYLON
For Pure and Applied Sciences (JUBPAS)
Special Issue 1: The First Babylon Conference on Countering Extremism and Terrorist Violence in Light of Global Political Shifts
Vol, 33; S.1 | 2025

الخلاصة

تبحث هذه الدراسة في الصراع المتصاعد بين ضرورة مكافحة المحتوى الإرهابي عبر الإنترنت والمبادئ الأساسية لحرية التعبير وحفظ المعرفة. فالنموذج الحالي لإدارة المحتوى وعلى الرغم من استجابته لتهديدات أمنية مشروعة الا انه يفرض خطرا كبيرا لم يتم بحثه بشكل كافي، وهو:الإبادة المعرفية المعلوماتية أي التقليل المنهجي من قيمة أنظمة المعرفة وإسكاتها وإفناؤها من خلال المحو الرقمي.

من خلال تحليل البنية التقنية للإشراف الخوارزمي والقوى الجيوسياسية التي تشكل سياسات المحتوى والأطر القانونية التي تحكم الخطاب عبر الإنترنت، فان الدراسة تسلط الضوء على أزمة التوازن بين الأمان الرقمي وحماية الحقوق الأساسية. ان إجراءات الرقابة المشددة قد تؤدي إلى آثار معاكسة سلبية مثل أن تؤدي عن غير قصد إلى تدمير أدلة حيوية على انتهاكات حقوق الإنسان وإسكات الروايات المضادة المشروعة وتآكل السجل الثقافي الرقمي.

تقوم الدراسة بتحليل المخاطر السيبرانية المرتبطة بالمحتوى الإرهابي، ونقد غموض الأنظمة الآلية وتحيزاتها ووضع تصور للإبادة المعرفية الرقمية كضرر بالغ الأهمية. وتختتم الدراسة باقتراح إطار متعدد الأطراف لحوكمة المحتوى بما يحافظ على الحقوق والدعوة إلى تحول نموذجي من الرقابة الفظة إلى التنظيم الدقيق الذي يوازن بين الإزالة الاستباقية والحفظ الأرشيفي القوي.

الكلمات المفتاحية: التهديدات السيبرانية، المخاطر ، المحتوى الارهابي، ابادة معلوماتية، رقابة، الارشيف الرقمي

1- المقدمة

في صيف عام 2014، تزامن صعود تنظيم الدولة الإسلامية (داعش) وسيطرته على مساحات واسعة من العراق وسوريا مع إطلاق حملة إعلامية عالمية غير مسبوقة في تطورها وحجمها. لقد أتقن التنظيم استخدام الإنترنت ومنصات التواصل الاجتماعي محولاً إياها إلى أداة مركزية لنشر رسائله المتطرفة من خلال إنتاج مقاطع فيديو عالية الجودة تحاكي أساليب الإنتاج السينمائي في هوليوود واستخدام مكثف لمنصات مثل تويتر ويوتيوب ونجح داعش في الوصول إلى جمهور عالمي بلغات متعددة. ولم تقتصر هذه الحملة على الدعاية فقط، بل امتدت لتشمل التجنيد المباشر والتخطيط للعمليات وبث الرعب عبر نشر مشاهد العنف المروعة. [1]-[2]

هذا المشهد يسلط الضوء بحدة على سمة الانترنت الحديث ومفارقته المركزية ودوره المزدوج كونه قناة للتمكين المعرفي والتواصل العالمي ومن ناخية اخرى كوسيلة للانتشار السريع للمحتوى الضار الذي تنشره جهات إرهابية غير حكومية. هذه المفارقة تضع الحكومات ومنصات التكنولوجيا في مواجهة تحدي أساسي يكمن في: تفادي الخطر الجسيم المتمثل بسماحية انتشار المحتوى الإرهابي دون رادع ،الامر الذي قد يؤدي إلى التطرف والعنف وإلحاق ضرر مجتمعي واسع النطاق، هذا من جانب ومن جانب اخر يبرز خطر الرقابة المفرطة التي قد تنتهك الحقوق الأساسية لحرية التعبير وتكوين الجمعيات. وبالتالي

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

Article
JOURNAL OF UNIVERSITY OF BABYLON
For Pure and Applied Sciences (JUBPAS)
Special Issue 1: The First Babylon Conference on Countering Extremism and Terrorist Violence in Light of Global Political Shifts
Vol, 33; S.1 | 2025

فإن الشركت وصانعي السياسات مدعوون جميعا لتحقيق توازن دقيق بين التنظيم الفعال لحماية الأمن العام وحماية المبادئ الديمقراطية الأساسية. [3]

تقدم هذه الدراسة حجة مركزية تفيد أن التدابير الحالية لمكافحة الإرهاب وخاصة الاعتماد المتزايد على إدارة المحتوى الآلية، تخلق خطراً عميقاً وغير مقصود يسمى: الإبادة المعرفية المعلوماتية.

بالاعتماد على مفهوم الإبادة المعرفية –أي الإفناء المنهجي للمعرفة– نفترض أن أدوات وسياسات الرقابة الرقمية تعمل كآليات لهذا المحو الرقمي وبداعي تطهير الفضاء الرقمي من المحتوى الضار، فإننا نخاطر بتدمير معلومات لا تقدر بثمن بما في ذلك أدلة على جرائم الحرب وسجلات تاريخية حيوية وأصوات مهمشة تسعى لمواجهة التطرف. [4]–[5]

تناقش هذه الدراسة أن هذا المحو المنهجي للمعرفة لا يمثل مجرد ضرر جانبي بل هو تهديد شامل للنسيج الرقمي للمجتمع.

2– المواد وطرق العمل

تعتمد هذه الدراسة على منهجية كيفية تستند بشكل أساسي إلى تحليل مضمون مجموعة واسعة من المصادر الأولية والثانوية ووثائق سياسية صادرة عن هيئات حكومية ومنظمات فضلا عن تقارير تقنية من شركات التكنولوجيا والمؤسسات البحثية بالإضافة إلى الأدبيات الأكاديمية في مجالات الأمن السيبراني ودراسات الإنترنت والعلاقات الدولية وحقوق الإنسان.

كما تستخدم الدراسة منهج دراسة الحالة (Case Study) كأداة تحليلية رئيسية مع التركيز على حالة الحذف الآلي واسع النطاق للمحتوى الرقمي الخاص بجرائم التنظيم الارهابي الداعشي في العراق بهدف توضيح المفاهيم النظرية المطروحة وتجسيد آثارها العملية على أرض الواقع.

يتيح هذا المنهج المتكامل فهماً عميقاً للتقاطعات المعقدة بين التكنولوجيا والسياسة والأخلاق في الية إدارة المحتوى عبر الإنترنت.

2–1 تحليل متعدد الأبعاد للمخاطر السيبرانية من المحتوى المتطرف

عند تحليل المخاطر الناتجة عن انتشار المحتوى الإرهابي عبر الإنترنت، يظهر بوضوح أنها لا تشكل تهديدات معزولة بل تمثل سلسلة مترابطة من التأثيرات التي تمتد عبر مجالات متعددة. في حالات كثيرة تبدأ نقطة الانطلاق من خلل تقني بسيط، كخادم غير مؤمَّن، إلا أن استغلال هذه الثغرة قد يستخدم لتحقيق أهداف ذات أبعاد سياسية أو جيوسياسية مثل تعطيل البنية التحتية الحيوية بدعم من جهات دولية. [6]–[8]

1– التداعيات الجيوسياسية والاقتصادية : أظهرت النتائج أن الهجمات السيبرانية الإرهابية لها تأثير سلبي ومباشر على تقييم سوق الأوراق المالية للشركات المستهدفة، مما يؤسس صلة واضحة بين النشاط الرقمي والضرر الاقتصادي الملموس. كما

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com
مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

أن التوترات الجيوسياسية تدفع الجهات الفاعلة التي ترعاها الدول إلى استهداف البنية التحتية الحيوية بشكل متزايد، مما يحول الفضاء السيبراني إلى ساحة جديدة للصراع الدولي. [7]

2- : **ناقل التهديد التقني:** تستخدم المنظمات الإرهابية مجموعة متطورة من التكتيكات والتقنيات بما في ذلك البرامج الضارة والتصيد الاحتيالي+ وهجمات حجب الخدمة بالإضافة إلى التقنيات الناشئة مثل الذكاء الاصطناعي لإنشاء التزييف العميق والتلاعب بالرأي العام. [9]،[14]

3- **التأثير المجتمعي** :بالإضافة إلى التهديدات المادية، هناك تأثير نفسي عميق يتمثل في التطرف عبر الإنترنت حيث تساهم خدمات "غرف الصدى" و"فقاعات الترشيح" في تضخيم وجهات النظر المتطرفة. كما ان التعرض المستمر للمحتوى العنيف يسبب صدمة نفسية ليس فقط للجمهور العام ولكن أيضًا لمشرفي المحتوى أنفسهم فيؤدي إلى تآكل الثقة المجتمعية [12]. هذا الهجوم، وإن بدأ في بعده التقني فيمكن أن يفضي إلى أزمات اقتصادية تشمل اضطراب الأسواق وتقويض الثقة العامة وتصاعد مشاعر القلق والخوف.

تبين هذه السلسلة من التفاعلات أن المعالجات الأحادية والمحدودة بنطاق تقني أو مؤسساتي ضيق لم تعد مجدية فعلى أرض الواقع تتوزع المعالجات الحالية على تقارير متفرقة: تقرير أمني يسلّط الضوء على نوع البرمجية الخبيثة المستخدمة، وتقرير من جهة صناعية يناقش كلفة الاختراق، وتحليل في مجال العلاقات الدولية يصف الحدث بوصفه عملًا عدائياً ترعاه دولة ودراسة نفسية ترصد أثر الهجوم على مشاعر الجمهور. غير أن هذه المعالجات ورغم تباين تخصصاتها، تتناول في جوهرها جوانب مختلفة لحالة واحدة متكاملة فالرؤية الأعمق هي أن هذه ليست أربعة أحداث منفصلة؛ إنها أربعة جوانب لحدث واحد معقد. فلا تقتصر مخاطر المحتوى الإرهابي على التهديدات التقنية بل تمتد لتشكل نظاما مترابطا من المخاطر الاقتصادية والجيوسياسية والمجتمعية التي تتطلب فهمًا شاملاً [15] جدول (1).

جدول (1): ابعاد المخاطر السيبرانية

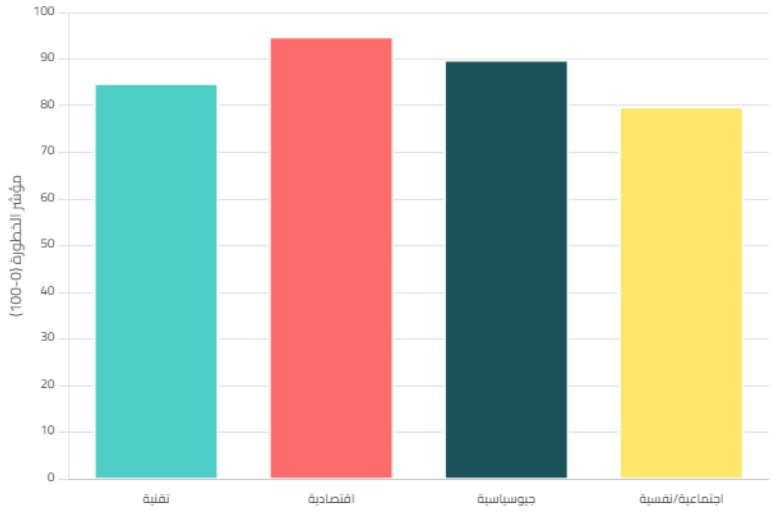
تهديدات تقنية	خسائر اقتصادة	صراع جيوسياسي	اثر مجتمعي
برمجيات خبيثة، تصيد، هجمات حجب الخدمة، وتزييف عميق تُستخدم لنشر الفوضى.	تأثير سلبي مباشر على أسواق الأسهم، تعطيل سلاسل الإمداد، وخسائر بمليارات الدولارات.	تسليح المعلومات، التجسس، وزعزعة استقرار الدول الخصوم عبر الفضاء الرقمي.	التطرف عبر الإنترنت، الصدمات النفسية، وتآكل الثقة المجتمعية بسبب الدعاية.

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com
مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

Article
JOURNAL OF UNIVERSITY OF BABYLON
For Pure and Applied Sciences (JUBPAS)
Special Issue 1: The First Babylon Conference on Countering Extremism and Terrorist Violence in Light of Global Political Shifts
Vol, 33; S.1 | 2025

وتكمن المشكلة الجوهرية في غياب رؤية شاملة تأخذ في الحسبان العلاقات البينية بين هذه الأبعاد. فبحسب تقرير المنتدى الاقتصادي العالمي، تبين إن أحد المحركات الأساسية لتعقيد مشهد الأمن السيبراني اليوم هو تنامي الترابطات داخل النظام البيئي الرقمي. وهذا ما يعزز الحاجة إلى تطوير نماذج تحليلية أكثر تكاملاً، تكون قادرة على محاكاة حلقات التأثير المتبادلة مثل العلاقة بين التوترات السياسية وتطور الهجمات، ثم أثر تلك الهجمات على الاقتصاد وانعكاساتها النفسية والمجتمعية وما تسببه من هشاشة في الثقة العامة قد تُستغل لاحقا من قبل أطراف متطرفة. [8] شكل (1)

يقارن المخطط ادناه بين الأبعاد المختلفة للمخاطر، موضحًا أن التأثيرات الاقتصادية والجيوسياسية قد تكون بنفس خطورة الهجمات التقنية المباشرة مما يؤكد الطبيعة المنهجية للتهديد.



شكل (1)

مستوى الخطورة النسبي

2-2 تحليل آليات وسياسات الإدارة الخوارزمية للمحتوى

اولا: الرقيب الآلي: البنية الداخلية لنظام المراقبة الرقمية

في ظل التزايد في حجم المحتوى الرقمي المنشور على الإنترنت، بات من المستحيل عمليا الاعتماد على العنصر البشري وحده في مراقبة كل ما يتم تداوله ونتيجة لذلك، تبنّت المنصات الرقمية تقنيات إشراف آلي تعتمد على الخوارزميات للقيام بمهام الرصد والتصفية حيث تعتمد هذه الأنظمة على منهجين رئيسيين يتكاملان فيما بينهما: المطابقة الرقمية والتنبؤ بالمحتوى المخالف [11].

- **المطابقة الرقمية** أو ما يُعرف بـ التجزئة الإدراكية والتي تقوم على إنشاء بصمة رقمية فريدة لكل محتوى سبق تصنيفه على أنه مخالف أو ضار، مثل فيديوهات التحريض على العنف أو المواد الإرهابية وتتيح هذه البصمات للخوارزميات التعرف

ISSN: 2312-8135 | Print ISSN: 1992-0652 | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com | info@journalofbabylon.com

السريع على أي نسخة مماثلة وحذفها تلقائيا. هذا الاسلوب يستخدم من قبل كبرى المنصات التقنية في إطار جهود جماعية لمكافحة المحتوى المتطرف. [11]

- **الأنظمة التنبؤية** تفتقر أنظمة المطابقة الرقمية اعلاه إلى القدرة على التعامل مع المحتوى المستجد فيظهر دور الأنظمة التنبؤية المعتمدة على الذكاء الاصطناعي والتعلم الآلي. وهذه النماذج تدرب على كميات ضخمة من البيانات لتتمكن من رصد أنماط معينة، وبالتالي التنبؤ بمدى احتمالية مخالفة المحتوى للسياسات، حتى وإن لم يكن مطابقًا لأي حالة سابقة. ووفقًا لتقارير رسمية من شركات مثل يوتيوب وفيسبوك، فإن ما يزيد عن 98% من المحتوى الإرهابي تتم إزالته بشكل استباقي، أي قبل أن يُتاح للمستخدمين. [11]

ورغم فعالية هذه الأنظمة من حيث السرعة والكمّ، إلا أن الاعتماد عليها يفتح الباب لتساؤلات أعمق تتعلق بالدقة، وشرعية القرار، وحدود السلطة التي باتت في قبضة الخوارزميات.

ثانياً: الية الصندوق الأسود ومشاكلها:

على الرغم من الكفاءة الظاهرية لهذه الأنظمة، إلا أنها تخلق مجموعة من التحديات العميقة التي تحول إدارة المحتوى من مجرد مشكلة تقنية إلى قضية سياسية وأخلاقية معقدة:

- **الغموض وانعدام الشفافية** :تعمل هذه الخوارزميات كـ "صناديق سوداء"، حيث تظل معاييرها وقواعد بياناتها سرية إلى حد كبير، مما يمنع التدقيق المستقل من قبل الباحثين أو المجتمع المدني.[11]

هذا الغموض يحرم المستخدمين من فهم سبب إزالة محتواهم فتصبح عملية الاستئناف شبه مستحيلة فيُخلق شعور بالعجز والظلم.

- **العدالة والتحيز الخوارزمي** :إن الأنظمة الآلية ليست محايدة بطبيعتها؛ فهي تعكس التحيزات الموجودة في البيانات التي تدربت عليها. هذا يمكن أن يؤدي إلى استهداف غير متناسب للمحتوى الذي تنتجه مجتمعات مهمشة أو إساءة تفسير اللهجات والسياقات الثقافية المختلفة.[11]

إن عجز الخوارزمية عن فهم "السياق" (ما يميز الحكم البشري) هو نقطة ضعفها الأساسية مما يؤدي إلى قرارات تفتقر إلى العدالة.

- **تجريد السياسة :(DE politicization)** ربما يكون هذا هو التحدي الأكثر خطورة. من خلال تقديم إدارة المحتوى كعملية تقنية وموضوعية، تتجنب المنصات الاعتراف بأن قراراتها هي في جوهرها قرارات سياسية. فتحديد ما الذي يشكل "خطاب كراهية" أو من هي "المنظمة الإرهابية" ليست قرارات تقنية، بل هي أحكام قيمية وسياسية عميقة. إن إخفاء هذه القرارات

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com
مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

داخل "الصندوق الأسود" للخوارزمية يسمح للمنصات بالتهرب من المساءلة العامة عن دورها كجهات فاعلة سياسية قوية تشكل الخطاب العالمي. [3]،[11]

ثالثاً: السيادة الرقمية: سباق تسلح عالمي للسيطرة على المحتوى

إن التحديات التي تطرحها إدارة المحتوى الخوارزمية لا تقتصر على سياسات الشركات ولكن تمتد إلى الساحة الجيوسياسية. فقد وجدت الدول الاستبدادية مثل روسيا والصين في نموذج "الرقابة الآلية" فرصة لتعزيز أجنداتها الخاصة بالسيطرة على الإنترنت تحت ستار أمن المعلومات. [10]

لاحظنا هنا ديناميكية مثيرة للقلق: فالأدوات والخطاب الذي طورته المنصات الغربية لمكافحة الإرهاب يتم استغلاله الآن من قبل الأنظمة غير الليبرالية لتبرير قمع المعارضة السياسية. فعندما تقوم منصة غربية بحذف ملايين المنشورات تلقائيا فإنها تخلق سابقة يمكن أن تستخدمها دولة استبدادية لتبرير حجبها للمحتوى الذي تعتبره مهددا للاستقرار الوطني. وبهذه الطريقة فإن الحل التقني الذي تم تصميمه لمشكلة محددة يوفر ومن غير قصد غطاءً من الشرعية لممارسات قمعية أوسع نطاق مما يساهم في تآكل فكرة الإنترنت المفتوح والعالمي. [10]

2-3 تحليل الإبادة المعرفية المعلوماتية كأثر جانبي للرقابة الآلية

في سعي الأنظمة لتحقيق الكفاءة وتقليل المخاطر على نطاق واسع تنتج بشكل منهجي شكلاً من أشكال المحو الرقمي الذي يدمر المعرفة الحيوية.

أولاً: من الإبادة المعرفية إلى الظلم المعرفي الرقمي

ينطلق تحليلنا من مفهوم "الإبادة المعرفية الذي صاغه علماء الاجتماع ونظرية ما بعد الاستعمار لوصف التدمير المنهجي لأنظمة المعرفة الخاصة بالمجتمعات المهمشة من قبل قوى مهيمنة.[4]

وفي العصر الرقمي، تتخذ هذه الظاهرة شكلاً جديداً، وهو ما نطلق عليه "**الإبادة المعرفية المعلوماتية**" هنا، تكون القوة المهيمنة بنية تحتية تقنية عالمية أي الخوارزميات التي تحكم منصات التواصل الاجتماعي. تعمل هذه الخوارزميات كحراس بوابة للمعرفة، حيث تحدد ما هو مرئي وما هو محذوف، ما هو شرعي وما هو ضار ليس بالضرورة ان يتم هذا المحو بنية خبيثة بل كنتاج ثانوي لنظام مصمم لتحسين متغيرات معينة (مثل تقليل المخاطر القانونية، وزيادة تفاعل المستخدمين). [4]،[5]

تتجلى هذه الإبادة المعرفية في الفضاء الرقمي عندما تقوم الخوارزميات بحذف شهادات الفيديو التي يرفعها ضحايا انتهاكات حقوق الإنسان لأنها تحتوي على عنف مصور، وبالتالي يتم التعامل مع شهادتهم على أنها محتوى ضار بدلاً من كونها

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com
مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

دليلاً.[10] . كذلك عندما يتم حذف الروايات المضادة التي تتحدى التطرف ولكنها تستخدم لغة أو صورًا تعتبرها الخوارزميات متطرفة فيُحرم المجتمع من الأدوات اللازمة لفهم ومواجهة الأيديولوجيات الخطيرة[11].

ثانياً: دراسة حالة: المحو المؤتمت لذاكرة العراق الرقمية

لتوضيح هذه الآليات عمليا، تناولنا حالة الحذف الآلي واسع النطاق للمحتوى الرقمي المتعلق بجرائم تنظيم داعش في العراق، ففي الوقت الذي كان فيه التنظيم الإرهابي ينشر دعايته الوحشية، كان هناك جهد موازٍ ومهم للغاية من قبل المواطنين العراقيين والصحفيين والمنظمات غير الحكومية لتوثيق هذه الجرائم. وتم تصوير مقاطع فيديو لمجزرة سبايكر، والتقاط صور لتدمير المواقع الأثرية في نينوى والموصل، وجمع شهادات الناجين في أرشيفات رقمية.[10] كان هذا المحتوى يمثل دليلاً حيوياً ورواية مضادة قوية لدعاية داعش.

ولاحظنا إن نفس الأنظمة الخوارزمية التي تم تصميمها لإزالة دعاية داعش وبسبب عدم قدرتها على التمييز بين السياقات أزالت أيضا كميات هائلة من هذا المحتوى التوثيقي، حيث تم حذف مقاطع الفيديو التي رفعها شهود عيان والصور التي التقطها الناجون والأرشيفات التي جمعها النشطاء، لأنها تحتوي على نفس المؤشرات البصرية أو الكلمات المفتاحية (مثل الأعلام السوداء ومشاهد العنف) التي تستخدمها الخوارزميات لتحديد المحتوى الإرهابي. [9]

في هذه الحالة، لم تفرق الخوارزمية بين الجاني الذي يصور جريمته للتباهي والضحية الذي يصور نفس الجريمة لتوثيقها وطلب العدالة، وهذا يمثل خسارة كارثية للأدلة الحاسمة لتحقيقات حقوق الإنسان والذاكرة التاريخية والمساءلة المستقبلية.[9]

ثالثاَ: منطق النظام: المحو سمة وليس خطأ

إن الإبادة المعرفية المعلوماتية ليست خللا عرضيا في نظام إدارة المحتوى بل هي سمة هيكلية ناشئة لنظام مصمم للتخفيف من المخاطر على نطاق صناعي حيث تواجه المنصات ضغوطا قانونية وتنظيمية وعامة هائلة لاتخاذ إجراءات حاسمة ضد المحتوى الإرهابي.[11]

في مواجهة الطوفان الهائل من المحتوى الذي ينشئه المستخدمون يوميا، تصبح المراجعة البشرية الشاملة ضربًا من المستحيل مما يجعل اللجوء إلى الأتمتة أمرًا حتميًا.[10] لكن هذه الأنظمة الآلية بطبيعتها تفتقر إلى الفهم البشري العميق للسياق وتعتمد على حسابات احتمالية. ومن أجل تقليل احتمالية تفويت محتوى ضار تتم معايرة هذه الأنظمة لتكون شديدة الحساسية، هذه الحساسية المفرطة حتما تؤدي إلى زيادة معدل عمليات الحذف الخاطئة.[11]

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com
مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

وضمن هذه المعادلة الصارمة يعامل مقطع فيديو يوثق جريمة حرب باعتباره مجرد بيانات ذات احتمالية عالية لاحتوائها على عنف مصور، وبالتالي يُصنف كمسؤولية قانونية يجب التخلص منها. أما قيمته كدليل أو كشهادة إنسانية أو كسجل تاريخي فهي ببساطة ليست متغيرات صُممت هذه الأنظمة لأخذها في الحسبان، ولهذا السبب، فإن تدمير المعرفة هنا هو النتيجة المنطقية والمتوقعة لنظام تم تحسينه في المقام الأول لضمان بقائه القانوني والتجاري، وليس للحفاظ على سجل البشرية الرقمي. [11]

3- النتائج والمناقشة: نحو إطار لحوكمة محتوى يحافظ على الحقوق

نقترح إطار متعدد الأوجه للتخفيف من خطر الإبادة المعرفية المعلوماتية مع الاستمرار في معالجة التهديدات الأمنية، فبدلا من الحذف الفوري نحتاج إلى نموذج جديد يوازن بين الإزالة الوقائية والحفظ الأرشيفي ويعزز الشفافية والمساءلة والإشراف البشري [10]، كما في شكل (2) . وهذا يجيب مباشرة على سؤال الدراسة لأخير.

3-1 الموازنة بين الإزالة الاستباقية والحفظ الأرشيفي:

- **الحلول التقنية:** ان التقنيات التي يمكن أن تساعد في تحقيق هذا التوازن:

1- **التجزئة الإدراكية للفرز، وليس الحذف:** ان مطابقة التجزئة الإدراكية لا ينبغي أن تؤدي إلى الحذف التلقائي بل يجب أن تبلغ عن المحتوى لمراجعة بشرية متخصصة أو توجيهه إلى أرشيف آمن ومقيد الوصول للتحقق منه من قبل كيانات موثوقة (مثل محققي حقوق الإنسان والأكاديميين). [10]

2- **العلامات المائية الرقمية لسلسلة العهدة:** استكشاف استخدام تقنيات العلامات المائية الرقمية لإنشاء سلسلة عهدة يمكن التحقق منها للمحتوى الذي يتم الحفاظ عليه كدليل. وهذا من شأنه أن يسمح بتوثيق المحتوى لاحقا مما يثبت أنه لم يتم العبث به. [12]

- **الحلول السياسية:** اقتراح سياسة النقل إلى الأرشيف، حيث لا يتم حذف المحتوى الذي تبلغ عنه الخوارزميات كدليل محتمل بشكل دائم ولكن يتم نقله إلى خزانة أدلة رقمية. ولا بد أن تُدار هذه الخزانة من قبل جهة خارجية موثوقة مثل تحالف من منظمات حقوق الإنسان المعتمدة أو مؤسسة أكاديمية مستقلة أو حتى هيئة تابعة للأمم المتحدة، لضمان الحياد ومنع إساءة الاستخدام من قبل الجهات الحكومية أو الخاصة. كما يجب أن يخضع الوصول إلى هذا الأرشيف لبروتوكولات قانونية وفنية صارمة لضمان عدم استغلاله لأغراض أخرى غير المساءلة القانونية والبحث الأكاديمي المشروع. [12]

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com
مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

JOURNAL OF UNIVERSITY OF BABYLON
For Pure and Applied Sciences (JUBPAS)
Special Issue 1: The First Babylon Conference on Countering Extremism and Terrorist Violence in Light of Global Political Shifts
Vol, 33; S.1 | 2025

شكل (2)

الاطار المقترح متعدد الاوجه لتقليل خطر الابادة المعلوماتية

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

3-2 ما وراء الأتمتة: الإشراف البشري الموثوق والنماذج المجتمعية:

في ضوء قصور الأنظمة الآلية الواضح يصبح من الضروري إعادة تأكيد الدور الذي لا غنى عنه للحكم البشري فالذكاء الاصطناعي وعلى الرغم من قدراته، هو عاجز عن فهم الفروق الدقيقة في السياق الإنساني.[12] وهنا تبرز أهمية تبني نهج الأمن السيبراني المرتبط بالإنسان وكما يدعو إليه المعهد الوطني للمعايير والتكنولوجيا والذي يهدف إلى تصميم أنظمة لا تسعى إلى استبدال الخبرة البشرية، بل إلى تعزيزها وتمكينها[12].

يتجاوز هذا المفهوم مجرد وجود إنسان في حلقة مراجعة قرارات الخوارزمية ليمتد إلى استكشاف نماذج حوكمة بديلة وأكثر شمولاً. فبدلاً من الاعتماد على نموذج مركزي للإشراف حيث يمكن استلهام حلول من الذكاء الجماعي.

إن نماذج مثل التنظيم المشترك والحوكمة متعددة الأطراف تفتح الباب أمام تقاسم المسؤولية بين المنصات والمستخدمين والمجتمع المدني والمؤسسات العامة. علاوة على ذلك تقدم نماذج الإدارة المجتمعية الناجحة التي نراها في منصات مثل "ويكيبيديا" دروسا قيمة في كيفية الاستفادة من الذكاء البشري الموزع والقادر على فهم السياق المحلي لإنشاء بيئة رقمية أكثر أمانا ومسؤولية[13].

4- الاستنتاج:

ان اسلوب مكافحة الارهاب الحالي عبر الإنترنت والذي تهيمن عليه الإدارة الخوارزمية الغامضة غير المعتمدة على السياق يؤدي الى إبادة معرفية معلوماتية، مما ينذر بخطر جسيم على التاريخ الرقمي والخطاب الحر.

يتطلب مواجهة التحدي المزدوج المتمثل في (مكافحة الإرهاب الرقمي وتجنب الإبادة المعرفية) استجابة منسقة ومتعددة الأطراف مع التركيز بشكل خاص على الابتكار في مجال التكنولوجيا وأمن المعلومات. لذلك ندعو الى االانتقال من نموذج الرقابة الآلية إلى النموذج المقترح المسؤول والمتمحور حول الإنسان. فمن الضروري التحول من سياسة الحذف الفوري إلى سياسة الإزالة إلى الأرشيف ليتم نقل المحتوى الحساس إلى خزانة أدلة رقمية" آمنة تقنيا، كما يمكن استخدام تقنية التجزئة الإدراكية للفرز بدلاً من الحذف والعلامات المائية الرقمية لضمان سلامة الأدلة.

5- التوصيات:

للوصول الى نموذج متكامل في حوكة العملية نقترح توصيات للجهات الفاعلة الرئيسية:

1- **للمنصات الرقمية: نحو حوكمة تقنية مسؤولة** تقع على عاتق المنصات المسؤولية الأساسية في إعادة تصميم بنيتها التحتية للأمن والثقة. وهذا يتطلب:

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

- **الحوكمة الفنية والشفافية:** يجب على المنصات تجاوز الأنظمة الغامضة الحالية من خلال تطبيق عمليات تدقيق تقنية منتظمة ومستقلة لخوارزميات الإشراف. الهدف من ذلك هو تحديد وتخفيف التحيزات الكامنة، ونشر تقارير شفافية تفصيلية توضح معدلات الخطأ (الإيجابيات والسلبيات الكاذبة) وفعالية المصنفات عبر مختلف اللغات والسياقات الثقافية.
- **الاستثمار في الذكاء الاصطناعي الواعي بالسياق** :يجب تخصيص موارد كبيرة للبحث والتطوير في الجيل القادم من نماذج الذكاء الاصطناعي القادرة على فهم السياق والنية بشكل أفضل. يتضمن ذلك التعاون مع الشركاء الأكاديميين ومنظمات حقوق الإنسان عبر بروتوكولات آمنة لمشاركة البيانات (مثل التعلم الفيدرالي) لتدريب النماذج على مجموعات بيانات أكثر تنوعًا وتمثيلاً.
- **هندسة أنظمة للحفظ:** يجب أن تتبنى المنصات مبدأ (الأمن حسب التصميم) الذي يشمل الحفاظ على المحتوى كجزء أساسي من دورة حياة البيانات، وهذا يعني دمج مسار عمل الإزالة إلى الأرشيف تقنيا واستخدام تقنيات الحفاظ على الخصوصية مثل التشفير المتماثل للسماح بتحليل البيانات المؤرشفة دون المساس بهويات الأفراد.

2- **لصانعي السياسات والهيئات التنظيمية: تشريع يواكب التكنولوجيا** يجب أن تتطور الأطر القانونية لتعكس الواقع التكنولوجي من خلال:

- **التنظيم المستنير تقنيًا** :يجب إصلاح الأطر القانونية التي تفرض مهلا زمنية قصيرة وصارمة للإزالة لأنها تجبر المنصات تقنيا على استخدام أنظمة آلية صارمة وعرضة للخطأ، اذ يجب أن يكون التشريع مرنا وأن يسمح بأنظمة استجابة متدرجة تتطلب المراجعة البشرية للحالات الحساسة للسياق.
- **تحفيز الابتكار الآمن:** يجب خلق حوافز قانونية ومالية للشركات التي تطور وتنشر تقنيات أمن معلومات متقدمة للحفاظ على المحتوى، يشمل ذلك تمويل الشراكات بين القطاعين العام والخاص التي تركز على إنشاء خزائن أدلة رقمية آمنة وقابلة للتشغيل البيني، وتطوير معايير قوية للعلامات المائية الرقمية لضمان سلامة المحتوى المؤرشف.

3- **للمجتمع المدني والمجتمع التقني:** يلعب المجتمع المدني دورا حيويا في الابتكار من خلال:

- **تطوير قدرات تقنية مستقلة:** من الضروري تطوير أدوات مفتوحة المصدر ومعايير لامركزية للحفاظ على الأدلة الرقمية كبديل من الاعتماد الكلي على البنية التحتية للشركات ويمكّن من التحقق المستقل.
- **بناء بروتوكولات آمنة لـ "المبلغين الموثوق بهم** : تفعيل العمل مع المنصات لإنشاء برامج مبلغين موثوق بهم فعالة وآمنة تقنيا، حيث يتضمن ذلك إنشاء واجهات برمجة تطبيقات (APIs) وقنوات آمنة تسمح بدمج مدخلات الخبراء من الصحفيين وباحثي حقوق الإنسان مباشرة في مسارات عمل الإشراف، مما يخلق آلية تجاوز للقرارات الآلية البحتة في الحالات عالية المخاطر.

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com
مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

Conflict of interest.

There is no conflict of interest

References

[1] J. M. Berger and J. Morgan, "The ISIS Twitter Census: Defining and Describing the Population of ISIS Supporters on Twitter," *The Brookings Project on U.S. Relations with the Islamic World*, Washington, D.C., Mar. 2015.

[2] C. Winter, "The Virtual 'Caliphate': Understanding ISIS's Propaganda Strategy," *The Tony Blair Institute for Global Change*, London, UK, May 2015.

[3] J. Zittrain, *The Future of the Internet—And How to Stop It*. New Haven, CT, USA: Yale University Press, 2008.

[4] B. de Sousa Santos, *Epistemologies of the South: Justice Against Epistemicide*. London, UK: Routledge, 2014.

[5] W. D. Mignolo, "Epistemic Disobedience, Independent Thought and Decolonial Freedom," *Theory, Culture & Society*, vol. 26, no. 7-8, pp. 159-181, 2009.

[6] K. T. Smith, L. M. Smith, M. Burger, and E. S. Boyle, "Cyber terrorism cases and stock market valuation effects," *Journal of Financial Crime*, vol. 30, no. 2, pp. 385-404, 2023. doi: 10.1108/JFC-09-2022-0210.

[7] H. Jamaluddin, "الأمن السيبراني والتحول في النظام الدولي" [Cybersecurity and the Transformation of the International System], *Majallat Al-Siyاسة/Al-Dawliyya*, vol. 24, no. 1, pp. 1-20, Jan. 2023.

[8] World Economic Forum, "Global Cybersecurity Outlook 2025," Insight Report, Geneva, Switzerland, Jan. 2025.

[9] S. Iftikhar, "Cyberterrorism as a global threat: a review on repercussions and countermeasures," *PeerJ Computer Science*, vol. 10, p. e1875, 2024. doi: 10.7717/peerj-cs.1875.

[10] D. Flonk, "Emerging illiberal norms: Russia and China as promoters of internet content control," *International Affairs*, vol. 97, no. 6, pp. 1925-1943, 2021. doi: 10.109/ia/iiab177.

[11] R. Gorwa, R. Binns, and C. Katzenbach, "Algorithmic content moderation: Technical and political challenges in the automation of platform governance," *Big Data & Society*, vol. 7, no. 1, 2020. doi: 10.1177/2053951719897945.

[12] J. Haney et al., "Workshop Summary Report for ConnectCon 2024: 'Minding the Gaps in Human-Centered Cybersecurity'," *NIST Special Publication (SP) 1332*, Gaithersburg, MD, USA, Apr. 2025. doi: 10.6028/NIST.SP.1332.

[13] G. K. Shahi, "TweetInfo: An Interactive System to Mitigate Online Harm," *arXiv preprint arXiv:2403.01646*, Mar. 2024.

[14] V. Koutsouvelis, S. Shiaeles, B. Ghita, and G. Bendiab, "Detection of Insider Threats using Artificial Intelligence and Visualisation," in *Proc. 2020 6th IEEE International Conference on Network*

Softwarization (NetSoft), Ghent, Belgium, 2020, pp. 450-454. doi: 10.1109/NetSoft48620.2020.9165337.

[15] A. DiGiovanni, "The Trauma of Content Moderation," *The Verge*, Dec. 2019. [Online]. Available: https://www.theverge.com/2019/12/17/21021009/content-moderation-trauma-ptsd-facebook-youtube-google-counseling-mental-health

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية جامعة بابل للعلوم الصرفة والتطبيقية

ISSN: 2312-8135 | Print ISSN: 1992-0652

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com