مجلة

تُعنى بنشر البحوث القانونية المتعلقة بتقنية المعلومات والذكاء الاصطناعي والعلوم المتقدمة

مجلة علمية محكمة | العدد (15) | السنة التاسعة | ذو القعدة 1443 هـ | يونيو 2022 م

ISSN 2312-5799

معهد دبي القضائي

المسؤول قانوناً عن استخدام الروبوتات في الأعمال العسكرية

المستشار الدكتور/ أبو بكر محمد الديب

جرائم الإرهاب السيبراني باستخدام الطائرات المسيّرة (الدرون) التحديات الأمنية واستراتيجية المواجهة

الدكتور/ عماد الدين محمد كامل عبد الحميد

دور الذكاء الاصطناعي في تحقيق العدالة الجنائية: التشريع الإماراتي نموذجاً

الدكتور/ محمد عبد الله العـوًا

www.dji.gov.ae

معهد دبي القضائي

مجلة علمية محكمة | العدد (15) | السنة العاشرة | ذو القعدة 1443 هـ | يونيو 2022م

رؤيتنا

أن نكون مركزًا إقليميًا للتميز القانوني والعدلي

رسالتنا

تزويد أعضاء المجتمع القانوني بأفضل تدريب مهني
والتطوير المستمر وإكسابهم المعرفة الحديثة ذات الصلة

معهد دبي القضائي
DUBAI JUDICIAL INSTITUTE

صندوق بريد: 28552 دبي
الإمارات العربية المتحدة
هاتف: 00971 4 20 54 112
00971 4 20 54 110
فاكس: 00971 4 28 27071
www.dji.gov.ae
research@dji.gov.ae

www. / DubaiJudicial

عن المجلة

«مجلة معهد دبي القضائي» تُعنى بنشر البحوث والدراسات القانونية المتعلقة بتقنية المعلومات والعلوم الحديثة، مجلةٌ علميَّةٌ مُحَكَّمةٌ تقبل النشر باللغة العربية، والإنجليزية، والفَرَنسية. يلفت مجال اهتمامها إلى طبيعة موضوعاتها حيث وُصِفتْ بحوثُها ودراستُها بالقانونية، وتعلَّقتْ بتقنية المعلومات والعلوم الحديثة.

وتتمثل موضوعاتها في المشكلات القانونية المعاصرة التي يتحتم بحثها في ضوء التقدم العلمي بطرفتيه: طفرة التقدم في مجال المعلومات وشبكة الاتصال، وطفرة التقدم في المجال البيولوجي.

لقد جاء عُنوانُ المجلة من السعة والشمول إلى حد كبير؛ لأن حصيلةَ التطورات العلمية سريعةٌ ومتنوعةٌ، ولا فكاكَ من أبعادِها وانعكاساتِها على كافة فروع القانون.

والمجلة تتضمن الأبواب الآتية:

- البحوث والدراسات القانونية.
- الاجتهادات القضائية وتشمل:
  - التعليق على الأحكام.
  - المبادئ القانونية التي يرسيها القضاء الإماراتي والقضاء المقارن.
- النصوص القانونية المستحدثة.
- التقارير العلمية عن الندوات والمؤتمرات وورش العمل.
- عرض الرسائل الجامعية والكتب.

أولوية النشر وترتيبه

- الموضوعات المرتبطة بدولة الإمارات العربية المتحدة.
- تاريخ وصول البحث إلى مدير تحرير المجلة.
- تنوع موضوعات البحث.
- ترتيب البحوث في المجلة يخضع لاعتبارات فنية.

الأهداف

1. تعزيز وتكريس ثقافة ومنهجية إجراء البحوث والدراسات القانونية المتعلقة بالذكاء الاصطناعي والعلوم المتقدمة.
2. إثراء العمل القضائي بالبحوث والدراسات القانونية التي تعكس التطور التشريعي المواكب للتقدم العلمي، ما يعين القاضي في أداء عمله وتوسيع مداركه وزيادة حصيلته المعلوماتية.
3. العمل على تنشيط الاجتهاد في مجال الفقه والقضاء من خلال نشر الدراسات والبحوث والمقالات المعمقة والتعليقات على الأحكام ذات الصلة بانعكاسات التقدم العلمي.
4. إمداد المحاكم والنيابات العامة بالبحوث والدراسات التي تسهم في تطوير القضاء في إطار تعاون مثمر بين الفقه والقضاء.
5. الاهتمام بالدراسة القانونية المقارنة للقوانين وأحكام القضاء للاطلاع على الخبرات الأجنبية وطريقة معالجتها للمشكلات القانونية الناتجة عن انعكاسات التقدم العلمي وتأثيره، مع مراعاة قيم المجتمع ومصالحه.
6. الاهتمام بدراسة التشريعات المكملة التي تعكس تجاوب المُشَرِّع مع التقدم العلمي بغرض رفع ما قد يكون من تناقض بين نصوصها أو بينها وبين غيرها من تشريعات، فالتحديث التشريعي لأي قانون يجب أن يكون نتاج تركيب علمي متناسق.
7. قيام المعهد بإحدى مهامه على وجه فعال وسريع في إمداد الدوائر المعنية بنتائج الدراسات والبحوث التي يمكن أن تفيد تلك الدوائر في تشخيص المشكلات التي يعكسها التقدم العلمي وتقديم الحلول المقترحة.. وبخاصة في حالات الاستعجال، حيث يلزم سرعة التدخل التشريعي تحت تأثيره.
8. إثراء المكتبة القانونية بصفة خاصة والمكتبة العربية بصفة عامة، ليس فقط بالبحوث والدراسات المتعلقة بتقنية المعلومات والعلوم الحديثة، بل وبنتائج هذه الدراسات وتقويمها في ضوء ما يسفر عنه التطبيق العملي.

قواعد النشر

النشر بالمجلة يتم وفقاً للقواعد التالية:

1. أن يتسم البحث بالعمق والأصالة والثراء المعرفي.
2. الالتزام بأصول البحث العلمي وقواعده العامة، ومراعاة التوثيق العلمي الدقيق.
3. يجب أن يكون البحث خاليًا من الأخطاء اللغوية والنَّحْوية، مع مراعاة الترقيم المتعارف عليه في الأسلوب العربي، وضبط الكلمات التي تحتاج إلى ضبط، وتقوم هيئة التحرير بالمراجعة اللغوية والتعديل بما لا يخل بمحتوى البحث أو مضمونه.
4. أن لا يكون البحث قد سبق نشره على أي نحو كان، أو تم إرساله للنشر في غير المعهد، ويثبت ذلك بإقرار من الباحث.
5. يقدم البحث عبر أحد العناوين الإلكترونية الخاصة بالمعهد أو بإدارة المعرفة والنشر.
6. ألا يزيد عدد صفحات البحث أو الدراسة على 50 صفحة من الحجم العادي (A4) وأن لا يقل عن 40 صفحة، ويجوز في بعض الحالات التغاضي الزيادة في عدد الصفحات إذا كان تقسيم البحث إلى قسمين أو أكثر يؤدي إلى الإخلال بوحدة البحث.
7. يلتزم الباحث بعدم إرسال بحثه إلى أية جهة أخرى للنشر حتى يصله رد المجلة.
8. يرفق الباحث بحثه بنبذة عن سيرته العلمية، وعنوانه بالتفصيل ورقم هاتفه، والفاكس (إن وجد) وبريده الإلكتروني.
9. تخضع البحوث التي ترد إلى المعهد للتقويم والتحكيم من قِبَل المختصين للحكم على أصالتها وجديتها وقيمتها وسلامة طريقة عرضها، ومن ثَمَّ صلاحيتها للنشر من عدمها.
10. يمنح كل باحث خمس نسخ من العدد المنشور فيه بحثه.
11. يمنح المعهد مكافأة مالية للأبحاث التي تقرر صلاحيتها للنشر ويقوم المعهد بنشرها.
12. تصبح البحوث والدراسات المنشورة ملكًا لمعهد دبي القضائي، ولا يحق للباحث إعادة نشرها في مكان آخر دون الحصول على موافقة كتابية من المعهد.
13. للمعهد الحق في ترجمة البحث أو أجزاء منه-متى اقتضتْ الظروف ذلك - بما لا يخل بمحتوى البحث، أو مضمونه، أو فحوى مادته العلمية.
14. أصول البحوث التي تصل إلى المجلة لا ترد سواء نشرت أو لم تنشر.
15. ترسل البحوث إلى مدير تحرير المجلة عبر البريد الإلكتروني research@dji.gov.ae أو على أحد العناوين الإلكترونية المثبتة بالمجلة.

المحتويات

كشاف أعداد المجلة

م	البحث	اسم الباحث	الصفحات		بيانات النشر	لغة النشر
			من	إلى		
1	المسؤولية المدنية الناشئة عن الجريمة المعلوماتية في القانون الدولي الخاص.	أ.د. أحمد محمد أمين الهواري	16	52	العدد الأول، السنة الأولى، جمادى الآخرة 1433هـ/ مايو 2012 م.	العربية
2	حجية المحررات الإلكترونية في الإثبات : تعليق على باكورة أحكام القضاء الدبوي.	أ.د. محمد محمد محمد أبوزيد	56	100	العدد الأول، السنة الأولى، جمادى الآخرة 1433هـ/ مايو 2012 م.	العربية
3	تعليق على قضاء دبي بشأن الاختصاص القضائي بجرائم الإنترنت	د. عبدالرازق الموافي عبداللطيف	104	137	العدد الأول، السنة الأولى، جمادى الآخرة 1433هـ/ مايو 2012 م.	العربية
4	النصوص القانونية المستحدثة: النصوص القانونية ذات الصلة بانعكاسات التقدم العلمي التي أدخلت على نصوص القوانين الرئيسة.	أ.د. محمد محمد محمد أبوزيد	140	147	العدد الأول، السنة الأولى، جمادى الآخرة 1433هـ/ مايو 2012 م.	العربية
5	دعوة المشرع لرفع التعارض بين ثبوت النسب بالبصمة الوراثية ونفيه باللعان	أ.د. محمد محمد محمد أبوزيد	16	33	العدد الثاني، السنة الأولى، ربيع الثاني 1424هـ/ مارس 2013 م.	العربية
6	عقد إيواء الموقع الإلكتروني: دراسة مقارنة	د. طاهر شوقي محمد محمود	35	77	العدد الثاني، السنة الأولى، ربيع الثاني 1424هـ/ مارس 2013 م.	العربية
7	التصويت الإلكتروني وأثره في ممارسة الديمقراطية	د. عبدالكريم محمد محمد السروي	78	137	العدد الثاني، السنة الأولى، ربيع الثاني 1424هـ/ مارس 2013 م.	العربية
8	قراءة في قانون مكافحة جرائم تقنية المعلومات لدولة الإمارات العربية المتحدة	د. عبدالرازق الموافي عبداللطيف	139	186	العدد الثاني، السنة الأولى، ربيع الثاني 1424هـ/ مارس 2013 م.	العربية
9	أضواء على نصوص المرسوم بشأن المسؤولية المدنية عن الأضرار النووية	أ.د. محمد محمد محمد أبوزيد	189	219	العدد الثاني، السنة الأولى، ربيع الثاني 1424هـ/ مارس 2013 م.	العربية
10	تأملات في أحكام سند الشحن البحري الإلكتروني (مقال)	المستشار الأمين عثمان إسماعيل	221	230	العدد الثاني، السنة الأولى، ربيع الثاني 1424هـ/ مارس 2013 م.	العربية
11	عقود التجارة الإلكترونية في القانون الدولي الخاص	أ.د. أحمد محمد أمين الهواري	15	72	العدد الثالث، السنة الثانية، ذو القعدة 1424هـ/ سبتمبر 2013	العربية
12	حماية المستهلك الإلكتروني في العقد الإلكتروني	أ.د. ماجدة شلبي	75	164	العدد الثالث، السنة الثانية، ذو القعدة 1424هـ/ سبتمبر 2013 م.	العربية
13	الرقابة على محتوى الإنترنت	د. طاهر شوقي مؤمن	167	206	العدد الثالث، السنة الثانية، ذو القعدة 1424هـ/ سبتمبر 2013 م.	العربية
14	باكورة الأحكام القضائية لمحكمة تمييز دبي في تطبيق تقنيات الاتصالات في قضايا الأحوال الشخصية	أ.د. محمد محمد محمد أبوزيد	209	217	العدد الثالث، السنة الثانية، ذو القعدة 1424هـ/ سبتمبر 2013 م.	العربية
15	حكم المحكمة الأمريكية العليا: تسريب معلومات سرية للتحايل في سوق الأوراق المالية	إعداد هيئة تحرير المجلة	219	232	العدد الثالث، السنة الثانية، ذو القعدة 1424هـ/ سبتمبر 2013 م.	العربية

م	البحث	اسم الباحث	الصفحات		بيانات النشر	لغة النشر
			من	إلى		
16	المبادئ الرئيسة للمسؤولية المدنية عن الأضرار النووية	د. محمد السيد الدسوقي	18	65	العدد الرابع، السنة الثانية، رمضان 1435هـ/ يوليو 2014م.	العربية
17	الجريمة المعلوماتية: دراسة مقارنة بين القانونين الليبي والإماراتي	د. رحاب علي عميش	66	103	العدد الرابع، السنة الثانية، رمضان 1435هـ/ يوليو 2014م.	العربية
18	تعليق على حكم محكمة القضاء الإداري المصرية في شأن حجب المواقع الإباحية	المستشار حسن البنا عبدالله عياد	104	145	العدد الرابع، السنة الثانية، رمضان 1435هـ/ يوليو 2014م.	العربية
19	حقوق البث الجزئي لمباريات كرة القدم فيما دون الوقت الكامل للمباراة	المستشار ستيوارت بيبوورث	146	158	العدد الرابع، السنة الثانية، رمضان 1435هـ/ يوليو 2014م.	العربية والإنجليزية
20	التخفي: نظرة متعمقة في شبكة تور (شبكة تخفي) وآثارها على أمن الحاسوب وحرية الرأي والتعبير في العصر الرقمي.	تشيلسي أيه لويس	24	107	العدد الخامس، السنة الثالثة، جمادى الأولى 1436هـ/ فبراير 2015م.	العربية والإنجليزية
21	المخاطر القانونية الدولية المتعلقة بالمصادر المفتوحة وحلولها المحتملة.	تشينج يو هو	111	163	العدد الخامس، السنة الثالثة، جمادى الأولى 1436 هـ / فبراير 2015م.	العربية والإنجليزية
22	تعليق حول حكم محكمة العدل الأوربية الصادر في 13 مايو 2014 بشأن الحق في اعتبار بعض الوقائع في طي النسيان.	الصالحين محمد العيش	168	178	العدد الخامس، السنة الثالثة، جمادى الأولى 1436 هـ / فبراير 2015م.	العربية
23	المسؤولية المدنية عن أضرار المنتجات الطبية المعيبة: دراسة مقارنة بين القانون الإماراتي والقانون الفَرَنسي.	د. رغيد عبدالحميد فتال د. أحمد سليمان	18	79	العدد السادس، السنة الثالثة، صفر 1436هـ/ ديسمبر 2015م.	العربية
24	القانون الواجب التطبيق على العقد الإلكتروني في التشريع الإماراتي.	د. زياد خليف العنزي	80	117	العدد السادس، السنة الثالثة، صفر 1436هـ/ ديسمبر 2015م.	العربية
25	شروط الإعلان التجاري عبر الإنترنت	د. طاهر شوقي مؤمن	118	143	العدد السادس، السنة الثالثة، صفر 1436هـ/ ديسمبر 2015م.	العربية
26	حكم وقتي بشأن تدابير وقتية وتحفظية، صادر من قِبَل رئيس لجنة الطعون التابعة لمحكمة التحكيم الرياضية في دعوى التحكيم رقم 3861/أ/ 2014، المنظورة أمام محكمة التحكيم الرياضية.	حكم تحكيم صادر من قِبَل محكمة التحكيم الرياضَية.	144	153	العدد السادس، السنة الثالثة، صفر 1436هـ/ ديسمبر 2015م.	العربية
27	دعوى التحكيم رقم 3488/ ت/ 2014، محكمة التحكيم الرياضية المرفوعة من قِبَل الوكالة العالمية لمكافحة المنشطات، ضد السيد/ جوها لا لوكَا.	حكم تحكيم صادر من قِبَل محكمة التحكيم الرياضَية.	154	193	العدد السادس، السنة الثالثة، صفر 1436هـ/ ديسمبر 2015م.	العربية

م	البحث	اسم الباحث	الصفحات		بيانات النشر	لغة النشر
			من	إلى		
28	دعاوى التحكيم: 3665 و3666 و3667 / ت / 2014 (محكمة التحكيم الرياضية) الدعوى المرفوعة من قبل لويس سواريز ونادي برشلونة لكرة القدم واتحاد أوروجواي لكرة القدم ضد الاتحاد الدولي لكرة القدم، حكم تحكيم صادر من قبل محكمة التحكيم الرياضية.	حكم تحكيم صادر من قِبَل محكمة التحكيم الرياضيَة.	194	227	العدد السادس، السنة الثالثة، صفر 1436هـ/ ديسمبر 2015م.	العربية
29	تدابير الأمم المتحدة لمكافحة استخدام الإنترنت لأغراض إرهابية: علاج جذري للمشكلة أم مجرد مسكن لها؟	د. ماهر إدريس البنا	18	48	العدد السابع، السنة الرابعة، شوال 1437هـ/ يوليو 2016م.	العربية والإنجليزية
30	مستقبل حقوق الملكية الفكرية في مجال اللوحات المقتبسة من صور	تشينج يو هو	50	94	العدد السابع، السنة الرابعة، شوال 1437هـ/ يوليو 2016م.	العربية والإنجليزية
31	حق الولي في إلزام الحاضنة بتمكينه من الرؤية الإلكترونية للمحضون عبر وسائل التواصل الاجتماعي.	أ.د. محمد عبدالرحمن الضويني	96	104	العدد السابع، السنة الرابعة، شوال 1437هـ/ يوليو 2016م.	العربية
32	التعدي على العلامة التجارية لوي فيتون	حكم صادر من محكمة استئناف الولايات المتحدة الأمريكية ـ الدائرة التاسعة	106	120	العدد السابع، السنة الرابعة، شوال 1437هـ/ يوليو 2016م.	العربية والإنجليزية
33	نزاع حول نطاق العلامة التجارية: Taylorgang .Com	مركز الويبو WIPO للتحكيم والوساطة	122	137	العدد السابع، السنة الرابعة، شوال 1437هـ/ يوليو 2016م.	العربية والإنجليزية
34	الشكلية الإلكترونية وحماية المستهلك في القانون الإماراتي والمقارن	أ.د. عابد فايد عبدالفتاح فايد	18	51	العدد الثامن، السنة الخامسة، ذو الحجة 1438هـ/ يوليو 2018م.	العربية
35	حماية المصنفات الرياضية وفقًا لقانون حقوق المؤلف والحقوق المجاورة الإماراتي رقم (7) لسنة 2002 والاتفاقيات الدولية ذات الصلة	د. عامر محمود الكسواني د. مراد محمود المواجدة	52	97	العدد الثامن، السنة الخامسة، ذو الحجة 1438هـ/ يوليو 2018م.	العربية
36	الأبعاد الدستورية للفضاء الإلكتروني: دراسة مقارنة	د. سيمون بدران	99	134	العدد الثامن، السنة الخامسة، ذو الحجة 1438هـ/ يوليو 2018م.	العربية
37	نزاع الطماطم	حكم المحكمة العليا بالولايات المتحدة الأمريكية	137	140	العدد الثامن، السنة الخامسة، ذو الحجة 1438هـ/ يوليو 2018م.	العربية والإنجليزية
38	الآثار القانونية للإنترنت على سيادة الدول: الاستقلالية الد ستورية نموذجًا.	د. سيمون بدران	21	55	العدد التاسع، السنة السادسة، ذو الحجة 1439هـ/ سبتمبر 2018م.	العربية

م	البحث	اسم الباحث	الصفحات		بيانات النشر	لغة النشر
			من	إلى		
39	بصمة المخ وبصمة الحامض النووي DNA: النظام الجنائي الإسلامي	د. الهاني طايع	57	116	العدد التاسع، السنة السادسة، ذو الحجة 1439 هـ / سبتمبر 2018 م	العربية
40	من الأحكام القضائية: حكم محكمة استئناف الولايات المتحدة الأميريكية الدائرة الثانية/ كريستيان لوبوتان إس إيه/ ضد/ إيف سان لوران أمريكا هولدينج: هل يصلح اللون الأحمر كعلامة تجارية؟.	حكم محكمة استئناف الولايات المتحدة الأميريكية الدائرة الثانية	119	148	العدد التاسع، السنة السادسة، ذو الحجة 1439هـ/ سبتمبر 2018م.	العربية والإنجليزية
41	من الرسائل العلمية الجامعية: ملخص مناقشة أطروحة الدكتوراه في القانون الجنائي المعنونة بالجرائم المرتكبة عبر وسائل التواصل الاجتماعي: دراسة مقارنة.	د. حوراء موسى	151	166	العدد التاسع، السنة السادسة، ذو الحجة 1439هـ/ سبتمبر 2018م.	العربية
42	الحماية القانونية للبريد الإلكتروني	أ.د. عابد فايد عبدالفتاح فايد	21	79	العدد العاشر، السنة السابعة، رجب 1440هـ/ مارس 2019م.	العربية
43	كاميرات المراقبة التلفزيونية المغلقة CCTV وسيلة للمراقبة السابقة على ارتكاب الجريمة لأغراض منع الجريمة وملاحقة مرتكبيها	أ.د. خالد موسى توني	81	131	العدد العاشر، السنة السابعة، رجب 1440هـ/ مارس 2019م.	العربية
44	اللوائح والقوانين المنظّمة للذكاء الاصطناعي	بقلم: كريستوفر فونزون وكيت هينزلمان	133	137	العدد العاشر، السنة السابعة، رجب 1440هـ / مارس 2019م.	العربية
45	تنظيم الذكاء الاصطناعي	بقلم: البروفيسور ديلاكروس	139	143	العدد العاشر، السنة السابعة، رجب 1440هـ / مارس 2019م.	العربية
46	الاتحاد الأوربي يناقش القضايا القانونية المتعلّقة بالذكاء الاصطناعي	بقلم: ديريك دو بريز	145	150	العدد العاشر، السنة السابعة، رجب 1440هـ / مارس 2019م.	العربية
47	التطبيب عن بعد: دراسة مقارنة بين القانون الفرنسي وقانون المسؤولية الطبية الإماراتي.	د. عمرو طه بدوي محمد	24	149	العدد الحادي عشرة، السنة الثامنة، شعبان 1441هـ/ أبريل 2020م.	العربية
48	قرار إداري رقم (30) لسنة 2017 باعتماد اللائحة التنظيمية لخدمات الرعاية الصحية عن بعد.	حميد القطامي، المدير العام رئيس مجلس إدارة هيئة الصحة بدبي.	150	177	العدد الحادي عشرة، السنة الثامنة، شعبان 1441هـ/ أبريل 2020م.	العربية
49	الذكاء الاصطناعي والقانون: لمحة عامة.	هاري سوردين	178	215	العدد الحادي عشرة، السنة الثامنة، شعبان 1441هـ/ أبريل 2020م.	مترجم عن الإنجليزية
50	استراتيجية الإمارات للذكاء الاصطناعي.		216	218	العدد الحادي عشرة، السنة الثامنة، شعبان 1441هـ/ أبريل 2020م.	العربية

م	البحث	اسم الباحث	الصفحات		بيانات النشر	لغة النشر
			من	إلى		
51	تقرير ختام ورشة عمل رسم مستقبل المعرفة القضائية المنجزات والتطلعات في الذكاء الاصطناعي.	معهد دبي القضائي	219	225	العدد الحادي عشرة، السنة الثامنة، شعبان 1441هـ/ أبريل 2020م.	العربية
52	نحو تنظيم قانوني لحوكمة إلكترونية للشركات العائلية وفقاً لقوانين دولة الإمارات العربية المتحدة: دراسة مقارنة.	د. أحمد مصطفى الدبوسي السيد	26	87	العدد الثاني عشرة، السنة الثامنة، شعبان 1441هـ/ أكتوبر 2020م.	العربية
53	هل سيؤدي كوفيد 19 إلى الاحتجاج بشرط القوة القاهرة؟	آن هنري وديفيد كيركباتريك	92	98	العدد الثاني عشرة، السنة الثامنة، شعبان 1441هـ/ أكتوبر 2020م.	مترجم عن الإنجليزية
54	أكبر خمس (5) قضايا بموجب قانون التكنولوجيا في العام 2016.		100	103	العدد الثاني عشرة، السنة الثامنة، شعبان 1441هـ/ أكتوبر 2020م.	مترجم عن الإنجليزية
55	حكم محكمة النقض الفرنسية أوبر ضد سائقيها		106	117	العدد الثاني عشرة، السنة الثامنة، شعبان 1441هـ/ أكتوبر 2020م.	مترجم عن الفرنسية
56	قانون رقم (9) لسنة 2020 م بشأن تنظيم الملكيّة العائليّة في إمارة دبي.	حكومة دبي	120	131	العدد الثاني عشرة، السنة الثامنة، شعبان 1441هـ/ أكتوبر 2020م.	العربية
57	عامل الوجوه التعبيرية: إضفاء الطابع الإنساني على قانون الخطاب الرقمي الناشئ.	إليزابيث أ. كيرلي. مارلين.م. ماكماهون.	26	80	العدد الثالث عشر، السنة التاسعة، رمضان 1442هـ/ أبريل 2021م.	العربية، مترجم عن الإنجليزية
58	مدى إمكانية منح الذكاء الاصطناعي حق براءة الاختراع عن ابتكاراته.	أحمد مصطفى الدبوسي السيد.	82	103	العدد الثالث عشر، السنة التاسعة، رمضان 1442هـ/ أبريل 2021م.	العربية
59	السوار الإلكتروني في دولة الإمارات العربية المتحدة: تطبيق ذكي وبديل عن العقوبة والحبس الاحتياطي.	د. عماد الدين محمد كامل عبدالحميد	27	58	العدد الرابع عشر - السنة التاسعة - ربيع الأول 1443 هـ / أكتوبر 2021م.	العربية
60	الالتزام بالتبصير الإلكتروني قبل التعاقد في العقود الإلكترونية: دراسة في القانون الإماراتي والمقارن.	أ.د. غازي خالد أبو عرابي	59	91	العدد الرابع عشر - السنة التاسعة - ربيع الأول 1443 هـ / أكتوبر 2021م.	العربية

تقديم

بقلم : القاضي الدكتورة ابتسام علي البدواوي
المدير العام-رئيس التحرير

يسرُّنا أن نضع تحت بصر القراء الأعزاء وبين أيديهم عددَنا الخامسَ عشر من مجلة معهد دبي القضائي والذي جاء زاخراً بأبحاثٍ قانونيةٍ في عالم التكنولوجيا والذكاءِ الاصطناعي التي تم تحكيمها تحكيماً معمى ، وإننا لنفخرُ باختيارِ الباحثين في مجالات القانونِ والعلومِ الحديثةِ مجلة المعهد للنشر فيها ، ويأتي هذا العدد ليضم في جَنَباته رؤياَ تعكس الثورة والمتغيرات التي طرأت على الساحة التكنولوجية والقانونية ، ويدل على ذلك البحث الأول الذي حدَّد فيه الباحثُ المسؤولَ قانوناً عن استخدام الروبوتات في الأعمالِ العسكرية، وأخطائِها ومخالفاتِها لقانون الحرب؛ وخَلُص في شأنِ ذلك إلى أنَّ الدولة هي المسئولةُ عن استخدامِ الأسلحةِ ذاتية التشغيل وهو ما تؤكد عليه قواعد المسئولية الدولية في العَديد من نصوصها والتي أشار إليها في متن دراسته ، أمَّا البحث الثاني ، فقد جاء بعنوان جرائم الإرهاب السيبراني باستخدام الطائرات المسيرة (التحديات الأمنية واستراتيجية المواجهة) جسد الباحث مشكلةَ بحثه في مجموعةٍ من الإشكاليات القانونية والفنية والأمنية المتعلقة بالإرهاب السيبراني وتحدياتِ الأمنِ القومي للدولِ نتيجة استخدام الطائرات المسيرة، وأوصى المُشرِّع الإماراتي باستحداثِ قانون اتحادي موحدَ يتناول تنظيم صناعةِ وانتاجِ واستخدام الطائراتِ المسيرةِ لمخاطرها على الأمن القومي ، وفي ختام عددنا جاء البحث الثالث ليزودنا بالمعرفة عن الذكاءِ الاصطناعي ودوره في تحقيق العدالة الجنائية (التشريع الإماراتي نموذجاً) ، وأشار الكاتب إلى اهتمامِ المُشرِّع الإماراتي بتقنينِ دور تقنيات الذكاءِ الاصطناعي لدعم اتخاذ القرار القضائي تحقيقاً للعدالة الجنائية وإنفاذ القانون ، ولفت الباحث عنايةَ أجهزةِ الشرطةِ إلى أنَّ استخدام الذكاءِ الاصطناعي سلاحٌ ذو حدين؛ فقد يُمكّن الجماعات الإرهابية من الهجماتِ الالكترونيةِ والاعتداءاتِ الجسديةِ عن طريقِ الطائرات المسيرةِ بدون طيار ، ونشرِ الأخبارِ الكاذبةِ فضلاً عن التزويرِ والتلاعبِ بالأدلةِ المقدمةِ للمحكمة .

وختاما ننقلُ لكتّابنا الأفاضل الشكرَ والتقدير لثقتهم واختيارهم مجلة معهد دبي القضائي لتكون المنبرَ المنفردَ والرائدَ لأعمالهم القانونية والشكرُ موصولٌ للسادةِ أعضاءِ الهيئةِ الاستشاريةِ للمعهد، وأعضاء هيئةِ التحريرِ لإسهاماتهم في استمراريةِ عملِ المجلة.

EaBadwawi@dji.gov.ae

المسؤول قانونًا عن استخدام الروبوتات في الأعمال العسكرية؟

بقلم

المستشار الدكتور/ أبو بكر محمد الديب

وزارة العدل – مصر

مجلة علمية محكمة | العدد (15) | السنة العاشرة | ذو القعدة 1443 هـ | يونيو 2022م

المسؤول قانوناً عن استخدام الروبوتات في الأعمال العسكرية

المستشار الدكتور/ أبو بكر محمد الديب

وزارة العدل – مصر

مقدمة

من أهم القضايا الناشئة عن الأتمتة المتزايدة [1] قضية المسؤولية عن الخسائر البشرية أو الأضرار أو الانتهاكات الأخرى لقوانين الحرب، وعند انتهاك هذه الحدود لاستخدام القوة من جانب القوات العسكرية أو قوات الشرطة التابعة للدول أو القوات المسلحة الأخرى، قد تكون الدول مسؤولة دولياً عن الأخطاء المرتكبة، ويمكن أن يتحمل الضباط - أو آخرون- مسؤولية جنائية فردية.

فاستخدام الروبوتات المقاتلة بشكل مستمر قد ينتج عنه خرق لبعض أحكام القانون الدولي، مما يفرض البحث عن أحكام المسؤولية القانونية [2] عن خرق هذه القواعد، بالإضافة إلى طرح حلول لإشكالية[3] إعمال قواعد المسؤولية عن انتهاك الروبوتات المقاتلة [4] لأحكام القانون الدولي الإنساني من تطلب أشخاص مسؤولين مباشرة عن تلك الجرائم المرتكبة بواسطتها.[5]

(1) تعني الأتمتة المتزايدة زيادة مستويات الأوتوماتيكية.

(2) Ugo Pagallo, the laws of robots: crimes, contracts and torts, law, governance and technology series, volume 10, 2013, Series Editors: Pompeu Casanovas and Giovanni Sartor, Springer Science+Business Media Dordrecht 2013, p29.

(3) إذ نودي بتزويدها بقدر من الوعي،

Nehal Bhuta, Antonino Rotolo and Giovanni Sartor, Awareness and Responsibility in Autonomous Weapons Systems, Department of Law, European University Institute, Florence, Italy, CIRSFID and Department of Legal Studies, University of Bologna, Italy, 2019. p.257.

وأضاف البعض الآخر أن تزويد الأسلحة بقواعد القانون الحرب لهو أهم خصيصة يمكن من خلالها تمكين الآلة من الإلمام بقواعد الحرب، ومن ثم المساعدة على تحميلها بالمسئولية.

Marc Cannellos and Rachel Haga, Lost in translation building a common language for regulating autonomous weapons, Published in IEEE Technology and Socitry Magazine, September 2016., p60

(4) Jonathan Crowe and Kylie Weston – Scheuber, Principles of International Humanitarian Law, Edward Elgar publishing Limited, 2013., p1.

(5) Danial N. Hammond, Autononomous Weapons and the Problem of Stste Accountability, Chicugho Journal of International law, volume 15, number 2, Article 8, 2015., p 669.

ويؤكد العمل الدولي[1] على ضرورة بناء قواعد المسؤولية الدولية قبل استخدام الروبوتات المقاتلة؛ ضماناً لعدم انتهاكها للقانون الدولي،[2] إذ يترتب على استخدام الروبوتات المقاتلة في القانون الدولي نوعان من الآثار، يتعلق الأول منهما بمقاضاة الدولة التي استخدمت هذا السلاح، وإلزامها بالتعويض[3] عن الأضرار التي أحدثتها، فإذا توفرت شروط [4] المسؤولية الدولية فلا بد أن تترتب عليها بعض الآثار في حق الدولة المنسوب إليها الفعل غير المشروع دولياً، وتتمثل أهم هذه الآثار في إصلاح الضرر[5] والترضية.[6]

فما هي مسؤولية الدول أو الأطراف في نزاع ما، والمقاتلين الأفراد حيال قرارات استخدام القوة بواسطة الروبوتات المقاتلة ؟

إذا كان لا بد لقيام المسؤولية الدولية[7] من وجود فعل غير مشروع دولياً، فإن ذلك الفعل يجب أن ينسب إلى الدولة كي ترتب مسؤوليتها عنه، ويعتبر القانون الدولي العام، بصفة عامة، أن الفعل ينسب إلى الدولة إذا كان صادراً عن السلطات المكونة لها والتي تتمتع باختصاصات بموجب القانون الداخلي.[8]

ويتحقق هذا الشرط أيضاً في حالة استخدام الروبوتات المقاتلة، حيث إن استخدامه يتم من قبل القوات المسلحة التابعة للدولة، والتي تعد إحدى هيئات الدولة التي تتصرف باسمها، وفقاً لاتفاقية لاهاي 1907،[9] وهو أيضاً ما نصت عليه المادة الحادية والتسعون من البروتوكول الإضافي

(1) CCW/MSP/2015/3 p19.

(2) Hin Yan Liu, Gorization and legality of autonomous remote weapons system, international review of the Red cross, volume 94, No: 886, summer 2012, p 650.

(3) د. أحمد أبو الوفا، النظرية العامة للقانون الدولي الإنساني في القانون الدولي وفي الشريعة الإسلامية، دار النهضة العربية، الطبعة الرابعة، 2019، ص 95.

(4) د. إبراهيم محمد العناني، القانون الدولي العام – الدولة، 2012 /2013، بدون ناشر، ص126.

(5) د. محمد صافي، القانون الدولي العام، دار النهضة العربية، 2019، ص 405.

(6) د. عثمان عبد اللطيف، الألغام الأرضية والمسئولية الدولية بين القانون الدولي العام والشريعة الإسلامية، والألغام الأرضية في الأراضي المصرية نموذجا، دراسة مقارنة، الطبعة الأولى، دار النهضة العربية، 2015، ص75، ود. صلاح الدين عامر، مقدمة لدراسة القانون الدولي العام، دار النهضة العربية، الطبعة الثانية، 2007، ص835.

(7) (Brownies, Principles of Public international law, (8th Edition), Edited by: James Crawford, Oxford University Press, 2012, p.430

(8) د.محمد حافظ غانم، الوجيز في القانون الدولي العام، دار النهضة العربية، 1979، ص101.

(9) Karen Parker, Memorandum on weapons and the laws and customs of war, Intrnational Educational Development, Humanitarian Law Project, May 1997, p.25.

الأول.[1]

وإذا كانت الدولة التي استخدمت روبوتات مقاتلة قد خالفت بذلك أحكام القانون الدولي، وكانت هذه المخالفة صادرة عن قواتها المسلحة، فإن الدولة المسؤولة يترتب عليها الالتزام بالتعويض عن الأضرار التي تسبب بها هذا السلاح، باعتبار أن قيام المسؤولية الدولية يرتب نشوء الالتزام بالتعويض عن كافة النتائج التي ترتبت على الفعل غير المشروع الذي ينسب إليها.

وإذ لم يقر المجتمع الدولي بالمسؤولية الجنائية إلا للأشخاص الطبيعيين الذين يرتكبون أفعالاً يعتبرها القانون الدولي جرائم دولية ومنها جرائم الحرب والجرائم ضد[2] الإنسانية، وعلى ذلك تنحصر مسؤولية الدولة المخالفة للقانون الدولي الإنساني في إطار المسؤولية المدنية، وتوجه المسؤولية الجنائية إلى الأشخاص الطبيعيين المنسوب إليهم ارتكاب العمل المخالف للقانون الدولي الإنساني كجريمة حرب.[3]

إشكالية البحث:

ظهرت في الآونة الأخيرة تطبيقات عديدة للذكاء الاصطناعي في مجالات الحياة المختلفة، سواء على الصعيد الداخلي أو الدولي، كما ظهرت تلك التطبيقات في مجالات سلمية وأخرى قتالية، وإذا كانت عواقبها أكثر خطورة في المجالات الحربية عنها في المجالات السلمية، بسبب طبيعة الحروب وما يعتريها من أعمال قتالية تستهدف في الأساس الظفر بالمعارك، مما يتيح للآلات المشغلة ذاتياً التعرض البدني للإنسان وبما يؤثر في البيئات المختلفة وما يصيب الأعيان والأشخاص بأضرار لا متناهية من جراء استخدام آليات عسكرية تعتمد على الذكاء الاصطناعي والتعلم الآلي، فهل يمكن تحميلها بالتزامات قانونية؟

وما هي سمات المسؤولية التي يمكن فرضها عند تشغيل الآليات التي تعتمد على الذكاء الاصطناعي في الأعمال القتالية؟ وما عناصر هذه المسؤولية؟

(1) بموجب القانون الدولي يعتبر التصرف الصادر عن أي هيئة من هيئات الدولة، سواء كانت عسكرية أو مدنية، هو تصرف صادر عن الدولة بشرط أن تكون هذه الهيئة تتصرف بصفتها الرسمية. وللتعليق على هذه المادة، انظر: د. مصطفى أحمد فؤاد، النظام القانوني الدولي، دار المطبوعات الجامعية، 2019. ص492 حاشية 1.

(2) حول تعريف الجرائم ضد الإنسانية وعناصرها وصورها، انظر: د. أبو الخير أحمد عطية، المحكمة الجنائية الدولية الدائمة، المحكمة الجنائية الدولية الدائمة- دراسة للنظام الأساسي للمحكمة وللجرائم التي تختص المحكمة بالنظر فيها، دار النهضة العربية، 1999، ص169وما بعدها.

(3) د. إبراهيم العناني، قمع انتهاكات القانون الدولي الإنساني، مقال منشور ضمن إصدار: القانون الدولي الإنساني- دراسات مقارنة بين الشريعة الإسلامية والقانون الدولي، سلسلة الكتب الإرشادية- العدد الثاني، دار الكلمة للنشر والتوزيع، بدون سنة نشر، ص272.

وما أوجه اختلافها عن مسؤولية البشر؟ وعلى وجه العموم يثور التساؤل هل يمكن إخضاع الأسلحة ذاتية التشغيل لقواعد المسؤولية الدولية؟

لا يمكن الإجابة عن هذا السؤال بالإيجاب ما لم يتم تحديد: " المسؤول عن أخطاء الروبوتات العسكرية ومخالفاتها لقانون الحرب".

أهمية البحث

تنص رؤية الجيش الأمريكي في يونيو 2018 على تجربة وتطوير أنظمة التحكم الذاتي والذكاء الاصطناعي والروبوتات"؛ لجعل الجنود أكثر كفاءة ولتقليل الاعتماد على اللوجستيات".[1]

ولما كان من غير العادل مساءلة الآلات ذاتها عن الأخطاء التقنية التي يترتب عليها ارتكاب جرائم بسبب استخدام الروبوتات أثناء القتال، كون القانون الجنائي لا ينطبق على غير العقلاء، مما يقتضي إيجاد آلية لمعالجة هذه الإشكالية؛ لإيجاد آلية لتحقيق المساءلة الفعالة عن الجرائم التي ترتكب بواسطة الأسلحة ،[2] وتعد مسؤولية الأفراد [3] والدول أمراً أساسياً لضمان المساءلة عن انتهاكات القانون الدولي لحقوق الإنسان والقانون الدولي الإنساني؛ لأن عدم التعهد بالمساءلة يضعف مستوى الردع والمنع، فيتدنى بذلك مستوى حماية المدنيين [4] وضحايا جرائم الحرب المحتملين.[5]

ومن المحتمل أن تؤدي الطبيعة المركبة لتكنولوجيا الروبوتات المستقلة القاتلة – وتعدد الجهات التي قد تكون معنية بقرار نشرها- إلى حدوث ثغرة أو فراغ فيما يتعلق بالمساءلة، وتشمل قائمة المرشحين لتحمل المسؤولية القانونية: الأشخاص الذين يعملون في البرمجة الحاسوبية،

(1) ناثالي جوبيرت، شبح الروبوتات القاتلة - استخدام الطائرات بدون طيار في الميدان، 18 حزيران (يونيو) 2013 الساعة 5:48 مساءً - تم التحديث بتاريخ 19 حزيران (يونيو) 2013 الساعة 7:42 مساءً متاح على:

http: //robots.blog.lemonde.frتاريخ الاطلاع: 31 ديسمبر 2020، الساعة4م.

(2) See, Nehal Bhuta, Antonino Rotolo and Giovanni Sartor, Awareness and Responsibility in Autonomous Weapons Systems, Department of Law, European University Institute, Florence, Italy, CIRSFID and Department of Legal Studies, University of Bologna, Italy, 2019, p257.

(3) حول مفهوم المسؤولية الدولية الجنائية للفرد، انظر: د. حنان محب حسن حبيب، العدالة الدولية ومسئولية الأفراد وفقاً لقواعد القانون الدولي العام، رسالة دكتوراه، كلية الحقوق - جامعة الزقازيق، 2014، ص 64.

(4) حول الشروط الواجبة في الجرائم ضد المدنيين، د. إسماعيل عبد الرحمن، الحماية الجنائية للمدنيين في زمن النزاعات المسلحة " دراسة تحليلية تأصيلية " ، الهيئة المصرية العامة للكتاب، 2007 ، ص403.

(5) CCW/MSP/2015/3 p.211.

وصانعي[1] المعدات الحاسوبية أو بائعيها، والقادة العسكريين ومرؤوسيهم الـذين ينشرون تلك المنظومات، والزعماء السياسيين.[2]

تمهيد وتقسيم:

يعد من أهم القضايا الناشئة عن حلول الآلة محل البشر في ساحات المعارك مسألة المسؤولية عن الخسائر البشرية أو الأضرار أو الانتهاكات الأخرى لقوانين الحرب.[3]

والمسؤولية الدولية، هي نظام قانوني بمقتضاه يلتزم[4] الشخص الدولي بتعويض الأضرار التي تصيب أشخاصاً قانونية أخرى جراء قيامه بعمل أو امتناع عن عمل غير مشروع دولياً، أو مشروع ولكنه يتسم بخطورة عالية أو يعبر عن خطأ في تنفيذ الالتزامات الدولية.[5]

ونموذج المسؤولية القانونية الدولية المتعارف عليه حتى الآن في القانون الدولي هو نموذج المسؤولية المدنية، أي المسؤولية المؤدية إلى التزام المسؤول بتعويض المضرور وجبر الضرر.

ويجمع الفقه الدولي على أن المسؤولية الدولية تؤسس على مجرد حدوث ضرر لشخص دولي نتج عن عمل أو امتناع عن عمل صدر عن شخص دولي آخر، وإسناد ذلك العمل إلى الشخص الذي صدر عنه، ويترتب على قيام المسؤولية الدولية التزام الدولة المسؤولة بتعويض الأضرار التي وقعت للمضرور.[6]

وعندما تُشغل الأجهزة الآلية بالتحكم عن بعد ويُتخذ القرار النهائي باستخدام القوة القاتلة من جانب بشر، فإن المسؤولية الفردية والقيادية عما ينتج من أضرار يمكن تحديدها بسهولة على وجه العموم،[7] مما يقتضي التعرض لتحديد المسؤول جنائياً عن الجرائم التي ترتكب بواسطة الأسلحة ذاتية التشغيل.

(1) من المسؤول المصنع أم المشغل أم المستخدم أم المبرمج؟ انظر: Marc cannellos and Rachel haga, op.cit, p.56.

(2) A/HRC/23/47 para 77.

(3) انظر مثلا: 7/2005/E/CN.4 و311/A/61 وAdd.6/14/A/HRC/14.

(4) فهي وفقا لبعض الفقه الدولي : " التزام الشخص الدولي طبقا للقانون الدولي بإصلاح الضرر لصالح شخص دولي آخر كان ضحية تصرف أو امتناع " انظر: د. إبراهيم أحمد خليفة، التنظيم الدولي، النظرية العامة للدولة – النظرية العامة للمنظمات الدولية- منظمة الأمم المتحدة- منظمة التجارة العالمية، دار المطبوعات الجامعية، 2020، ص127.

(5) د. محمد صافي، المرجع السابق، ص344.

(6) د. أبو الخير أحمد عطيه، الالتزام الدولي بحماية البيئة البحرية من التلوث، كلية الحقوق- جامعة عين شمس، 1995، ص 269.

(7) A/65/321 para 33.

وتعرف الروبوتات[1] الحربية في نظرنا بأنها "أداةٌ ميكانيكية متحكم فيها بالحاسب الآلي الذي سبقت برمجته، ويمتلك العديد من درجات الحرية المبرمجة لأداء العديد من المهام الحربية.

فمن يكون المسؤول [2] إذا قتل جهاز آلي مدنيين في انتهاك للقانون الدولي الواجب التطبيق؟ هل هو المبرمج الذي صمم البرنامج الذي يحكم تصرفات الجهاز الآلي، أو المسؤولون العسكريون الذين ربما كانوا قد وافقوا على البرمجة، أو القائد البشري الذي أسندت إليه المسؤولية عن ذلك الجهاز، أو الجندي الذي ربما كان باستطاعته أن يمارس إشرافاً عليه ولكنه اختار ألا يفعل ذلك؟

وما الحال إذا كان القتل يعزى إلى عطل من نوع ما؟ أتكون الحكومة التي نشرت الجهاز الآلي هي المسؤولة، أم يكون المسؤول هو المهندس أم الصانع[3] الرئيسي، أم الفرد الذي تعود إليه المسؤولية النهائية عن البرمجة، أم شخص آخر؟

وما مستوى الإشراف الذي يتعين أن يمارسه الإنسان على الجهاز الآلي كي يكون مسؤولاً عن تصرفاته؟ وهل بالوسع تصور ظروف يمكن فيها بشكل مشروع برمجة أجهزة آلية كي تتصرف في انتهاك للقانون الدولي، أو هل يمكن[4] برمجتها في المقابل، بحيث تتجاهل التعليمات التي تعتبرها-في ظل الظروف المعنية- انتهاكاً لذلك القانون؟

وهل توجد أوضاع يكون من الملائم فيها استنتاج أنه ليس هناك فرد مسؤول، على الرغم من الحقيقة الواضحة التي تقول: إن أفعالاً غير قانونية قد أفضت إلى حدوث وفيات في صفوف المدنيين أو غيرهم؟

وتساءلت منظمة هيومان رايتس ووتش عمن سيتحمل مسؤولية الأفعال غير القانونية التي يرتكبها الروبوت، "وتتضمن الخيارات: القائد العسكري الذي وضع الروبوت في الميدان، والمبرمج، والمُصنع، والروبوت ذاته، ولكن كلها خيارات غير مرضية، فسيكون من الصعب -بل من غير العدالة- تحميل أول ثلاثة أطراف المسؤولية وعدم إيقاع العقوبة بالطرف الذي ارتكب الجريمة

(1) Ian GR Shaw, Robot Wars: US Empir and geopolitics in the robotic age, article in security dialogue, vol. 48(5), 2017., p 451.

(2) Hin Yan Liu, Gorization and legality of autonomous remote weapons system, international review of the Red cross, volume 94, No: 886, summer 2012, p650.

(3) فيما يتعلق بتحديد المسؤولية في ذات الإطار عن استخدام الألغام، د. إيناس مصطفي محمود أبوريه، المسئولية الدولية عن زراعة الألغام في ضوء أحكام القانون الدولي والإنساني، دار النهضة العربية، 2015، ص 316.

(4) ذهب ماركوساسولي إلى أن الروبوتات إذا كانت قادرة على التمييز بين الأوامر القانونية وغير القانونية، وقادرةً على تطبيق القانون على موقف معقد دون تدخل بشري، فسيكون من السهل برمجتها على عدم اتباع الأوامر غير القانونية، وإذا لم تتمكن من هذا فلا يجوز استخدامها، غير أنه لا يمكننا الزعم بحلول الروبوتات محل البشر في تحمل المسؤولية. ماركوساسولي، الأسلحة ذاتية التشغيل والقانون الدولي الإنساني: مزايا وأسئلة تقنية مطروحة ومسائل قانونية يجب توضيحها - بحث منشور ضمن إصدار اللجنة الدولية للصليب الأحمر بالقاهرة "القانون الدولي الإنساني في النزاعات المسلحة المعاصرة" 2017 ، ص151.

فعليًا وهو الروبوت ".[1]

ولما كان من المحتمل أن ينتهك استخدام الروبوتات المقاتلة قواعد القانون الدولي الإنساني، فإن استخدامه لا يرتب المسؤولية الدولية التقليدية، التي يعتبر التعويض عن الضرر الذي يسببه هذا السلاح نتيجة طبيعية لها فحسب، وإنما يمكن أن يترتب على استخدامه نتيجة أخرى وهي المسؤولية الجنائية الدولية عن هذا الاستخدام.

وعلى ذلك فإن تحديد المسؤولين عن انتهاكات الروبوتات المقاتلة لقواعد الحرب إذا ما خاضوها يسلتزم:

تحديد المسؤول جنائياً عن انتهاكات الروبوتات العسكرية لقواعد الحرب.

تحديد المسؤول مدنيا عن انتهاكات الروبوتات العسكرية لقواعد الحرب.

ونتناولها على النحو التالي:

المبحث الأول:
تحديد المسؤول جنائياً عن انتهاكات الروبوتات العسكرية لقواعد الحرب.

المبحث الثاني:
تحديد المسؤول مدنياً عن انتهاكات الروبوتات العسكرية لقواعد الحرب.

(1) انظر: ماركوساسولي، المرجع السابق، ص 235.

المبحث الأول

تحديد المسؤول جنائياً عن انتهاكات الروبوتات العسكرية لقواعد الحرب

أصبحت جرائم التكنولوجيا كثيرة ومتعددة، لذلك ابتكرت الحلول التكنولوجية المناسبة للتغلب على هذه الجرائم المستحدثة، إلا أن القوانين الحالية لا تستطيع التعامل مع هذه الجرائم،[1] لكن منظومة السلاح الآلي تعمل دائمًا في حدود برنامجها الذي صممه لها البشر،[2] لذا ذهب البعض إلى قصر المسؤولية الجنائية على الشخص الطبيعي وحده ،[3] إذ لا يخضع للقواعد القانونية إلا البشر، وفي حالة الروبوتات المقاتلة يخاطب القانون الدولي الإنساني البشر الذين يبتكرونها وينتجونها ويبرمجونها، وكذا من يقررون استخدامها ،[4] مما يقتضي تحديد دور كل من المشاركين في اتخاذ القرار للوقوف على مسؤوليته الجنائية.[5]

ومن الممكن معاملة الشخص الذي يتعمد برمجة منظومة - يستخدمها مسؤول تشغيل بحسن نية أثناء نزاع مسلح- على عدم الامتثال للقانون الدولي الإنساني على أنه المرتكب غير المباشر لجريمة الحرب المرتكبة أثناء النزاع، وثمة خيار آخر يتمثل في اعتبار المبرمج ضامنًا ملزمًا بالتدخل وقت الحرب لتجنب ارتكاب انتهاكات للقانون الدولي الإنساني، وبالتالي يكون قد ارتكب جريمة حرب من باب التقصير في حالة عدم تدخله، ومن الواضح أن مسؤول التشغيل إذا كان على دراية بالخلل الموجود في السلاح، فإن المبرمج سيكون عاملاً مساعداً على ارتكاب جريمة الحرب في هذه الحالة.[6]

لكن الروبوتات لا تملك إرادة أو أي وازع أخلاقي، لذلك لا يمكن تحميلها المسؤولية بأي طريقة من الطرق المعترف بها إذا ما تسببت في سلب الأرواح الذي يستدعي المساءلة عادة، حال ما إذا

(1) د. شريف درويش اللبان، تكنولوجيا الاتصال، المخاطر والتحديات والتأثيرات الاجتماعية، سلسلة العلوم والتكنولوجيا، الدار المصرية اللبنانية، 2008، ص 161.

(2) Final report of defense Defense science board, U.S. Department of Defense, Task Force Re-Port: The Role of Autonomy in (DOD) systems, 1, 21 (July 2012, P572.

(3) د. إسماعيل عبد الرحمن، المرجع السابق، ص272.

(4) ماركوساسولي، المرجع السابق، ص283.

(5) Nehal Bhuta, Antonino Rotolo and Giovanni Sartor, op.cit, p259.

(6) ماركوساسولي، المرجع السابق، ص152.

كان العنصر البشري هو المسؤول عن القرارات، فمن يتحمل المسؤولية إذن [1] ؟

لا يمكن الاحتجاج بأن النظام القانوني لقيام المسؤولية الدولية الجنائية بشكله الحالي يصعب انطباقه على استخدام منظومات الأسلحة المستقلة تماماً، بدعوى عدم مقبولية منح الآلة شخصية قانونية افتراضية تمكنها من تحمل المسؤولية واكتساب الحقوق، أو الاحتجاج بعدم توفر العمل الإجرامي والقصد الجنائي في حق الآلة، فالقانون الدولي الإنساني يخاطب في حالة الأسلحة ذاتية التشغيل البشر الذين يبتكرونها وينتجونها ويبرمجونها وكذلك من يقررون استخدامها.[2] وعلى ذلك لا بديل – في نظرنا- عن مسؤولية البشر.

فمنظومة السلاح الآلي تعمل دائماً في حدود برنامجها الذي صممه البشر[3] لها، فالإنسان هو[4] الذي يتخذ قراراً بتصنيع الآلة وتحديد المسؤول عن تصنيعها، وحتى إذا جاء يوم صممت فيه الروبوتات روبوتات أخرى فستظل هناك حاجة إلى إنسان ليطور الروبوت الأول ويصدر له تعليمات بشأن كيفية تصميم روبوتات جديدة، وهذا الإنسان مقيد بالقانون، أما الآلة فهي غير مقيدة بالقانون ،[5] وعلى ذلك، يظل الإنسان هو الجدير بتحمل المسؤولية الجنائية دون الآلة على الإطلاق.

ويمكننا استعارة نظرية الحراسة من القانون المدني، بحيث يكون الإنسان الذي يتولى السيطرة الفعلية على السلاح الذاتي "الأقل فتكاً" أو صاحب الدور البشري الفعال هو المسؤول جنائياً عما يرتكب بواسطة الروبوت من أفعال تشكل جرائم جنائية. و يغدو – أيضاً- من أطلق السلاح الذاتي "المستقل الفتاك" من البشر، أو من طور روبوتاً قادرا على إطلاقه هو المسؤول جنائياً – دون غيره – عن جميع الجرائم الخطرة التي تنتج عن إطلاقه، كما يعد مصدر الأمر باستخدام هذه الأسلحة ومن أطلقها بالفعل مسؤولاً جنائياً إذا توفرت جميع عناصر المسؤولية الجنائية.

(1) CCW/MSP/2015/3 p21.

(2) مما يبطل الحجة التي سيقت لامتناع تحقق المسئولية الجنائية، ومفادها أن المسئولية المباشرة أو التي تقع على عاتق الشخص الذي يسحب الزناد ويطلق النار لن تتحقق إلا بتوافر ثلاثة شروط، يتعلق الأول بالقصد الجنائي للروبوت، ويقتضي الثاني ضرورة تعديل النطاق الشخصي للمحاكم الجنائية الدولية وإضفاء الشرعية عليه، ويستلزم الثالث معاقبة مرتكب الجريمة وهو الروبوت الفاقد للإحساس والإدراك، ماركوساسولي، المرجع السابق، ص151.

(3) أشار مؤتمر الخبراء غير الرسمي 2016 إلى استكشاف النهج البديلة، التي تحدد الأسلحة ذاتية التشغيل في علاقاتها بالعنصر البشري المشغل ومستوى سيطرة المشغل وتأثيره على منظومة معينة. CCW/CONF.V/2 p8

(4) Final Report of the Defense Science Board (DSB) Task Force on: the Role of Autonomy in Department of Defense (DoD) Systems, Chairman, DSB: Dr. Paul Kaminski, Department of Defense, Defense Science Board, (July 2012).

(5) ماركوساسولي، المرجع السابق، ص 149.

مسؤولية الشركات المصنعة والمبرمجة:

تحمِّل القوانين الجنائية الوطنية- في أغلب الأحوال- المسؤولية الجنائية لمن يشيد - عمدًا أو استهتارًا أو إهمالًا - مبانٍ أو آلات معيبة تؤدي إلى خسارة في الأرواح البشرية ،[1] لكن البعض يذهب إلى أن امتلاك الآلة القدرة على إصدار قرار مستقل يهدم العلاقة السببية التي تسمح بإسناد الأفعال وتحديد المسؤولية ،[2] باعتبار أن البشر هم دائمًا من يحددون كيفية التصرف بموجب هذا الاستقلال، مما يؤكد ضرورة صياغة معايير محددة للعناية الواجبة بحيث يتقيد بها المصنعون والقادة على حد سواء.

لكننا نرفض القول بأن قدرة الآلة على اتخاذ قرار مستقل يهدم علاقة السببية، إذ من شأن مسايرته التضحية بالعدالة وبمعاقبة المسؤولين الأصليين عن الانتهاكات الجسيمة لقواعد الحرب، بالإضافة إلى إعطاء الضوء الأخضر للمطورين بإطلاق عنان الآلية نحو آفاق قد يعجز البشر عن مواجهتها دون رادع من قانون أو أخلاق.

المبحث الثاني

تحديد المسؤول مدنياً عن انتهاكات الروبوتات العسكرية لقواعد الحرب

في إطار تحديد الشخص المسؤول عن الضرر[3] ترى منظمة هيومان رايتس ووتش أن من غير الواضح من سيتحمل مسؤولية الأفعال غير القانونية التي يرتكبها الروبوت: "إذ تتضمن الخيارات: القائد العسكري[4] الذي وضع الروبوت في الميدان، والمبرمج والمُصنع والروبوت ذاته، فلا بد من

(1) من يعارض تحميل المنتج مسؤولية جنائية لم يوضح من يتحمل المسؤولية الجنائية إذا كان القائد ومسؤول التشغيل يعتقدان- خلافاً للواقع- أن المنظومة بُرمجت بالشكل الصحيح.

Michael N. Schmitt & Jeffrey S. Thurnher, “Out of the Loop”: Autonomous Weapon Systems and the Law of Armed Conflict, Harvard National Security Journal (2013), 231, 242–43. p279.

(2) ماركوساسولي، المرجع السابق، ص149.

(3) انظر: د. جمال عبد الفتاح عثمان، المسئولية الدولية عن عمليات البث المباشر العابر للحدود، في ضوء أحكام القانون الدولي "دراسة مقارنة" 2009، دار الكتاب القانوني، ص 369، د. أبو الخير أحمد، الالتزام الدولي بحماية البيئة البحرية والمحافظة عليها من التلوث، مرجع سابق، ص362.

(4) حول مسؤولية القائد العسكري، انظر: د. محمد عبد الكريم عزيز، مسئولية المقاتل عن انتهاك القانون الدولي الإنساني، الطبعة الأولى، مركز الدراسات العربية، 2017 ، ص253.

وجود شخص تنسب إليه المسؤولية على فرض وجود مسؤولية حتى قبل الآلة.[1]

إلا أنه سيكون من الصعب - بل من غير العدل- تحميل أول ثلاثة أطراف[2] المسؤولية وعدم إيقاع العقوبة بالطرف الذي ارتكب الجريمة فعليًا وهو الروبوت" ،[3] فمن المحتمل أن تؤدي الطبيعة المركبة لتكنولوجيا الروبوتات المستقلة القاتلة - وتعدد الجهات التي قد تكون معنية بقرار نشرها- إلى حدوث ثغرة أو فراغ فيما يتعلق بالمساءلة.

وتشمل قائمة المرشحين لتحمل المسؤولية القانونية: الأشخاص الذين يعملون في البرمجة الحاسوبية، وصانعي المعدات الحاسوبية أو بائعيها، والقادة العسكريين ومرؤوسيهم الذين ينشرون تلك المنظومات، والزعماء السياسيين.[4]

فمع حلول الآلة محل البشر في ساحات القتال، قد يصبح من الصعب تطبيق إطاري مسؤولية الدولة ومسؤولية الفرد،[5] فمن يكون المسؤول[6] إذا قتل جهاز آلي مدنيين[7] في انتهاك للقانون الدولي الواجب التطبيق؟ هل هو المبرمج الذي صمم البرنامج الذي يحكم تصرفات الجهاز الآلي، أو المسؤولون العسكريون الذين كانوا ربما قد وافقوا على البرمجة، أو القائد البشري الذي أسندت إليه المسؤولية عن ذلك الجهاز، أو الجندي الذي كان ربما باستطاعته أن يمارس إشرافاً عليه ولكنه اختار ألا يفعل ذلك؟

وما الحال إذا كان القتل يعزى إلى عطل من نوع ما؟ أتكون الحكومة التي نشرت الجهاز الآلي هي المسؤولة، أم يكون المسؤول هو المهندس أم الصانع الرئيسي، أم الفرد الذي تعود إليه المسؤولية النهائية عن البرمجة، أم شخص آخر؟

وما مستوى الإشراف الذي يتعين أن يمارسه الإنسان على الجهاز الآلي كي يكون مسؤولاً عن تصرفاته؟ وهل بالوسع تصور ظروف يمكن فيها بشكل مشروع برمجة أجهزة آلية كي تتصرف في انتهاك للقانون الدولي، أو هل يمكن برمجتها، في المقابل بحيث تتجاهل التعليمات التي تعتبرها

(1) Hin Yan Liu, op.cit, p 650.

(2) حول أطراف المسئولية، انظر: د. د.هشام عمر أحمد الشافعي، المسئولية الدولية عن الأضرار الناجمة عن الأنشطة الفضائية النووية، شركة الدليل للدراسات والتدريب وأعمال الطباعة والنشر، 2013 ، ص10. د. عصام زناتي، المسؤولية الدولية عن الأضرار الناجمة عن الأجسام الفضائية، دار النهضة العربية، 2003/2002، ص40.

(3) ماركوساسولي، المرجع السابق، ص149.

(4) CCW/MSP/2015/3 p21 - Marc cannellos and Rachel haga, op.cit, p.56.

(5) حول مركز الفرد في القانون الدولي، انظر: د. حنان محب، المرجع السابق، ص 68.

(6) د. عصام زناتي، المرجع السابق، ص46.

(7) Nicholas tsagourias and Alasdair Morrison, international humanitarian law, Cases, Materials and Commentary, Cambridge University Press, Online publication date: August 2018, P.110.

في ظل الظروف المعنية، انتهاكاً لذلك القانون؟ وهل توجد أوضاع يكون من الملائم فيها استنتاج أنه ليس هناك فرد مسؤول، على الرغم من الحقيقة الواضحة التي تقول أن أفعالاً غير قانونية قد أفضت إلى حدوث وفيات في صفوف المدنيين أو غيرهم؟[1]

عُرضت آراء مختلفة - في إطار العمل الدولي- بشأن مدى إمكانية مساءلة البشر عن أفعال منظومات الأسلحة ذاتية التشغيل، وقيل بأن تسلسل القيادة العسكري الحالي يمكن أن يضمن المساءلة، ويمكن للتدريب والتعليمات السليمة وقواعد الاشتباك أن تساعد أيضاً في تجنب إساءة استخدام المنظومات ذاتية التشغيل، وأُطلقت دعوات لوضع المزيد من الضمانات من أجل ضمان فعالية سلسلة المساءلة.[2]

لكن الروبوتات لا تملك أي وازع أخلاقي، ولذلك لا يمكن تحميلها المسؤولية بأي طريقة من الطرق المعترف بها إذا ماتسببت في سلب الأرواح الذي يستدعي المساءلة عادةً متى كان العنصر البشري هو المسؤول عن القرارات، فمن يتحمل المسؤولية إذن؟[3]

في الأساس لا يخضع للقواعد القانونية إلا البشر، وفي حالة الأسلحة ذاتية التشغيل، يخاطب القانون الدولي الإنساني البشر الذين يبتكرونها وينتجونها ويبرمجونها وكذلك من يقررون استخدامها، واعتبر الفرق بين منظومة الأسلحة والإنسان ليس فرقًا في الكم بل في الكيف، فالاثنان لا يخضعان لمعايير التقييم ذاتها بل يقع كل منهما في مستوى مختلف عن الآخر، وإذا كان البعض قد اعتبر لهذا السبب أن تزويد الأسلحة بقدر من الوعي[4] وإلمامها بقواعد القانون الحرب لهو أهم خصيصة يمكن من خلالها تحميلها بالمسؤولية [5] فإننا لا نقبل هذا الرأي ولو طرح لمعالجة فجوة المسؤولية وإشكالياتها مع صعوبتها.

فالمقاتل[6] إنسان، وهو وحده المخاطب بالالتزامات القانونية، ومهما تطور[7] الذكاء الاصطناعي في المستقبل، فسيكون هناك دائمًا إنسان في نقطة البداية،[8] فسيبقى الإنسان هو المسؤول عن التصرف والسلاح مجرد أداة، وإذا كانت الدولة المتحاربة تقف موقف المتهم، فعلى المرء أن

(1) A/65/321 para 34.

(2) CCW/MSP/2015/3 para 56.

(3) A/HRC/23/47 para76.

(4) Nehal Bhuta, Antonino Rotolo and Giovanni Sartor, op.cit, p.257.

(5) Marc cannellos and Rachel haga, op.cit, p.49.

(6) حول مفهوم المقاتل تفصيلا، انظر: د. مصطفي أحمد فؤاد، القانون الدولي الإنساني، دار المطبوعات الجامعية، 2019، ص184.

(7) انظر د. أسماء السيد محمد، ود. كريمة محمود محمد، تطبيقات الذكاء الاصطناعي ومستقبل تكنولوجيا التعليم THE Future of instructional Technology & Artificial Intelligence Applications - المجموعة العربية للتدريب والنشر، 2020، ص19.

(8) ماركوساسولي، المرجع السابق، ص 235 و277.

ينظر إلى الموضوع في إطار مسؤولية الدولة، والقاعدة المقررة التي تقضي بأن الدولة المتحاربة مسؤولة عن جميع الأعمال التي ارتكبها الأشخاص التابعون لقواتها المسلحة تمتد - بلاشك - إلى اختيار الأسلحة وطريقة استعمالها.[1]

كما أن البشر وحدهم هم القادرون على اتخاذ قرارات خاصة بالسياق تتعلق بالتمييز والتناسب واتخاذ الاحتياطات في أثناء القتال، وهم أيضاً القادرون على التصرف بناءً على الأخلاق والتمسك بالمسؤولية الأخلاقية وإظهار الرحمة والشفقة، بينما ليس بمقدور الآلات أن تزن الأمور بنفس الملكات البشرية المركبة والفريدة اللازمة في ميدان المعركة حتي تمتثل للقانون الدولي الإنساني، ولكونها أجساماً جامدة فهذه الآلات لن تحظي أبداً بملكة مثل الضمير البشري ولن تطور قيماً أخلاقية.[2]

وطرح البعض إسناد المسؤولية عن الأضرار المدنية إلى المُبرمِج والشركات المصنعة، وذلك بإقرار نظام يشبه النظام المتبع لتقرير المسؤولية المطلقة عن المُنتج، إلا أن القوانين الوطنية لم تتبن إلى الآن تحديد نطاق المسؤولية فيما يتعلق بالروبوتات وصناعتها، مما يثير التساؤل حول الشخص المسؤول، هل هو الروبوت المستقل القاتل الذي يشترك في إنتاجه واستخدامه عدد كبير من الناس؛ بيد أنه من المستبعد أن يكون شخص واحد من بين من اشتركوا في انتاجه "المُبرمج، والمُنتج، المستخدم" هو وحده فقط من يكون محيطاً بالتفاعلات المعقدة بين العناصر المكونة للروبوتات المستقلة.

ووفقاً لأصحاب هذا الرأي، يتحمل المنتج المسؤولية عن أخطاء التصنيع والبرمجة التي أدت إلى انتهاكه لقواعد القانون الإنساني وتحقيق الضرر، أو عدم تمكن المشغل من وقف الأضرار وإيقاف التشغيل في الوقت الملائم، وهكذا تعد الشركة المصنعة والمبرمجة مسؤولة قانوناً عن أي انتهاك لأحكام القانون الدولي الإنساني فيما يتعلق بالأسلحة ذاتية التشغيل، إذ يتعين على تلك الشركات مراعاة أحكام القانون الدولي الإنساني، خاصة وأنها من تقوم بإنشاء تلك الاسلحة وعلى معرفة كاملة بأهم خصائصها ومزاياها، وفي حال حدوث أضرار جراء استخدام تلك الأسلحة يمكن الرجوع على هذه الشركات بالتعويض.[3]

وطرح البعض فكرة المسؤولية التضامنية بين جميع الفاعلين - ومن بينهم الآلة- كوسيلة للتغلب

(1) فريتس كالسهوفن، الاتفاقية الخاصة بالأسلحة التقليدية "المبادئ القانونية التي بنيت عليها الاتفاقية "المجلة الدولية للصليب الأحمر، السنة الثالثة، نوفمبر/ ديسمبر، العدد السادس عشر، 1990، ص 485.

(2) الأسلحة ذاتية التشغيل - ضرورة اتفاق الدول على معنى السيطرة البشرية فعليا، اللجنة الدولية للصليب الأحمر. منشور على :
https://www.icrc.org/ar/autonomous-weapons-states-must-agree-what-human-control-means-practice ،

(3) Danial N. Hammond, op.cit, p665.

على احتمالية وجود فراغ في المسؤولية، على سند من وجود عدة مشغلين يتفاعلون سويا لإتمام مهمتهم، ومن ثم بات من الواجب عدم إفراد كل من الفاعلين بدور مستقل، وإنما تغليب النظر إلى المهمة كاملة والمحصلة النهائية إلى السلوك المشترك والنتيجة التي تم تحقيقها في إطار المنظومة وتم انهاؤها بفضل كل الفاعلين، وعلى ذلك لا يمكن قصر المسؤولية على أي منهم.[1]

ويقترح جانب من الفقه فرض ضريبة على مثل هذه الشركات تحصل لصالح الضحايا وفرض تأمين إجباري لتغطية المخاطر وسداد التعويضات عن وجود انتهاكات، إذ أن إعمال قواعد المسؤولية القانونية على الشركات المصنعة والمبرمجة من شأنه إجبار الشركات على العدول عن القيام بمشروعات تطوير الأسلحة المستقلة الفتاكة، والقيام بالتجارب التي تكفل الحد من الانتهاكات التي تحدث من استخدام مثل هذه الأسلحة.[2]

وفي النهاية وبالنظر إلى أحكام المسؤولية الدولية للدولة مقارنة بأحكام المسؤولية القانونية أو الجنائية للفرد، لا تثير مسؤولية الدولة جدلاً كبيراً، خاصة أن الدولة تعد المسؤول الأول عن استخدام الأسلحة ذاتية التشغيل، كما أن إعمال قواعد المسؤولية الدولية يؤكد مسؤولية الدولة، فالدولة هي المسؤول الأول والأوحد عن استخدام تلك الأسلحة.

(1) Nehal Bhuta, Antonino Rotolo and Giovanni Sartor, op.cit, p.257.

وعلى ذلك، نادت دراسات عربية بضرورة اعتماد وسائل كفيلة بالحد من الأخطاء والرعونة ولزوم وجود تحكم دائم ومستمر طوال الوقت في عمل الآلة والالتزام بالقواعد الأخلاقية والقانونية، ونادى أيضاً بوجود وعي ذاتي لهذه الأسلحة يتم تفعيله رغم مشاركة البشر في المسؤولية وذلك في إطار متطلبات التكامل، حيث سيتحول الإنسان إلى مراقب أكثر منه مشغلا للآلة.

(2) Danial N Hammond, op.cit, p667.

نتائج

تتحمل الدولة المسؤولية القانونية والسياسية عما تقوم به منظومات الأسلحة الذاتية التشغيل التي تستخدمها قوات هذه الدولة، على أن قيام المسؤولية الدولية التقليدية على عاتق الدولة التي تستخدم هذا السلاح، لا يؤثر في قيام المسؤولية الدولية الجنائية، أي أن المسؤوليتين تتقرران معاً، وهو ما أكدته المادة الحادية والتسعون من البروتوكول الإضافي الأول لعام 1977، وتم التأكيد عليه أيضاً في المادة 4/25 من النظام الأساسي للمحكمة الجنائية الدولية 1998، حيث نصت على أنه "لا يؤثر أي حكم في هذا النظام الأساسي يتعلق بالمسؤولية الجنائية الفردية".

ولا يمكن الاحتجاج بأن النظام القانوني لقيام المسؤولية الدولية الجنائية بشكله الحالي يصعب انطباقه على استخدام منظومات الأسلحة المستقلة تماماً، بدعوى عدم مقبولية منح الآلة شخصية قانونية افتراضية تمكنها من تحمل المسؤولية واكتساب الحقوق، أو الاحتجاج بعدم توفر العمل الإجرامي والقصد الجنائي في حق الآلة، فالقانون الدولي الإنساني يخاطب في حالة الأسلحة ذاتية التشغيل البشر الذين يبتكرونها وينتجونها ويبرمجونها وكذلك من يقررون استخدامها، وعلى ذلك لا بديل – في نظرنا- عن مسؤولية البشر.

لهذا الغرض تطالب المنظمات غير الحكومية على الأخص بإبقاء سيطرة بشرية هادفة على منظومات الأسلحة، ويعني هذا اتخاذ التدابير اللازمة التي من شأنها ضمان تنفيذ الآلة للمهام وفقاً لقصد القائد، والحفاظ على الموثوقية والشفافية، وإمكانية التنبؤ بالنتيجة المنشودة، والقدرة على التدخل ضمن الوظائف الحرجة في اختيار الأهداف ومشاركتها في الوقت المناسب، وفهم المسارات والقيود القانونية بما يتيح - في الأخير- تحميل القادة المسؤولية عن أي انتهاك قد يحدث.

مما يقتضي تأكيد الحفاظ على الدور البشري ودعم المشاركة البشرية وعدم الاستجابة لدعاوى خفض دور البشر وتزويد الآلة بالوعي.

توصيات

من الواجب أن يحصل المستخدمون على التدريب الملائم، وأن يخضعوا لآليات المساءلة، وهو ما يستلزم من مستخدمي منظومات الروبوتات المحاربة الاحتفاظ بسجلات، إلا أن المساءلة يجب أن تُطبق على المنتجين بالدرجة ذاتها، مع ضرورة وجود معايير مهنية متفق عليها، ونظراً للتطور الدائم في نظام هذه الأسلحة وارتكابها أفعالاً تشكل جرائم خاضعة لمظلة القانون الدولي الجنائي القاصرة قواعده عن مساءلة غير الطبيعيين، مما يستلزم المضي قدماً في خلق قواعد من شأنها تقرير مسؤولية تتناسب مع الطبيعة غير البشرية للسلاح، خاصة أن المعالجة الحالية للتهديدات التي تشكلها هذه الأسلحة تتم في التصدي لها من خلال القواعد التقليدية والإطار الأخلاقي وحده

وهو غير كاف، من ذلك تقرير المسؤولية الجنائية الفردية.

وتحث الدراسة على فرض ضريبة على الشركات المصنعة والمطورة تتضاعف كلما زادت مستويات الاستقلالية في عمل الروبوتات، وعلى منح إعفاءات ضريبية للشركات التي تقوم بتجارب مجدية في إطار تعظيم قواعد القانون الدولي الإنساني، وتهيئة الأسلحة ذاتية التشغيل للامتثال لتلك القواعد، ومضاعفة تلك الإعفاءات بزيادة مستويات التحكم البشري والحد من الاستقلالية، ومراعاة اعتبارات الشفافية في الإنتاج والتطوير، التي يناط برقابتها هيئة دولية متخصصة تنشأ لهذا الغرض.

ويجب أن تُكفل وفقاً للقانون الدولي الساري المساءلة عن تطوير ونشر واستخدام أي منظومة أسلحة ناشئة، من خلال كفالة تشغيل هذه المنظومات ضمن سلسلة قيادة وسيطرة مسؤولة يضطلع بها الإنسان، بحيث يبقى الإنسان مسؤولاً عن قرارات استخدام منظومات الأسلحة، ومراعاة هذا الأمر في كامل دورة حياة منظومة الأسلحة.

قائمة المراجع:

مراجع عربية:

1. د. إبراهيم أحمد خليفة، التنظيم الدولي، النظرية العامة للدولة – النظرية العامة للمنظمات الدولية- منظمة الأمم المتحدة- منظمة التجارة العالمية، دار المطبوعات الجامعية، 2020.
2. د. إبراهيم العناني، قمع انتهاكات القانون الدولي الإنساني، مقال منشور ضمن إصدار: القانون الدولي الإنساني- دراسات مقارنة بين الشريعة الإسلامية والقانون الدولي، سلسلة الكتب الإرشادية- العدد الثاني، دار الكلمة للنشر والتوزيع، بدون سنة نشر.
3. د. أبو الخير أحمد عطيه،
   - الالتزام الدولي بحماية البيئة البحرية من التلوث، كلية الحقوق- جامعة عين شمس، 1995.
   - المحكمة الجنائية الدولية الدائمة، المحكمة الجنائية الدولية الدائمة- دراسة للنظام الأساسي للمحكمة وللجرائم التي تختص المحكمة بالنظر فيها، دار النهضة العربية، 1999.
4. د. أبوبكرمحمد الديب، التطبيقات العسكرية للذكاء الاصطناعي في ضوء القانون الدولي العام، دار النهضة العربية-مصر 2021.
5. د.أحمد ابو الوفا،
   - النظرية العامة للقانون الدولي الإنساني في القانون الدولي والشريعة الإسلامية، دار النهضة العربية، الطبعة الرابعة، 2019.

- المسئولية الدولية للدول واضعة الألغام في الأراضي المصرية، "دراسة في إطار القواعد المنظمة للمسئولية الدولية وللألغام البرية" دار النهضة العربية، 2003/1423.
6. د.أحمد حشمت أبوستيت، نظرية الالتزام في القانون المدني الجديد، مطبعة مصر، الطبعة الثانية، 1954.
7. د.أحمد عبيس نعمة الفتلاوي، مشكلة الأسلحة التقليدية بين جهود المجتمع الدولي والقانون الدولي العام، منشورات زين الحقوقية – بيروت، 2013.
8. د. أحمد عطا عبد العظيم عبد اللطيف، المسئولية الدولية عن جريمة الإبعاد أو النقل القسري للمدنيين في ضوء أحكام القانون الدولي العام، كلية الحقوق- جامعة المنوفية، 2015.
9. د. أحمد محمد عفيفي أبو الفتوح طاحون، الجوانب القانونية للمنازعات المسلحة غير الدولية في ضوء قواعد القانون الدولي، رسالة دكتوراه، كلية الحقوق- جامعة المنوفية، -1438 2017.
10. ادوين وايز، تكنولوجيا صناعة الإنسان الآلي- الروبوت- دار الفاروق للاستثمارات الثقافية، 2008.
11. د. أسماء السيد محمد، ود. كريمة محمود محمد، تطبيقات الذكاء الاصطناعي ومستقبل تكنولوجيا التعليم THE Future of instructional Technology & Artificial Intelligence Applications - المجموعة العربية للتدريب والنشر، 2020.
12. د. إسماعيل عبد الرحمن، الحماية الجنائية للمدنيين في زمن النزاعات المسلحة " دراسة تحليلية تأصيلية "، الهيئة المصرية العامة للكتاب، 2007.
13. د. إيناس مصطفي محمود أبوريه، المسئولية الدولية عن زراعة الألغام في ضوء أحكام القانون الدولي والإنساني، دار النهضة العربية، 2015.
14. د.براء منذر كمال عبد اللطيف، الطائرات المسيرة من منظور القانون الدولي الإنساني، بحث منشور بمجلة العلوم الإنسانية، 2016.
15. د. جمال عبد الفتاح عثمان، المسئولية الدولية عن عمليات البث المباشر العابر للحدود، في ضوء أحكام القانون الدولي" دراسة مقارنة " 2009، دار الكتاب القانوني.
16. جون ماري هنكرتس، ولويز دوزوالد- بك، القانون الدولي الإنساني العرفي، اللجنة الدولية للصليب الاحمر، المجلد الأول، القواعد، 2016.
17. حماية ضحايا الحرب، إعداد: اجتماع فريق الخبراء الدولي الحكومي المعني بحماية ضحايا الحرب، جنيف، أبريل/ نيسان 1994، المجلة الدولية للصليب الأحمر، س7، العدد التاسع والثلاثون، سبتمبر/ أيلول- أكتوبر/ تشرين الأول، 1994.
18. د. حنان محب حسن حبيب، العدالة الدولية ومسئولية الأفراد وفقاً لقواعد القانون الدولي العام، رسالة دكتوراه، كلية الحقوق - جامعة الزقازيق، 2014.
19. د.رضوي عمار، المسئولية الدولية للشركات العسكرية والأمنية الخاصة خلال عمليات السلام، المجلة المصرية للقانون الدولي، المجلد الحادي والسبعون، 2015.
20. د. سما الشاوي، استخدام سلاح اليورانيوم المنضب في ضوء قواعد القانون الدولي، دار وائل للنشر والتوزيع، الأردن، الطبعة الأولي، 2014.
21. د.شريف أحمد عبد العزيز الشريف، الحماية الدولية للأعيان الثقافية في ظل الظروف الاستثنائية، رسالة دكتوراه، كلية الحقوق- جامعة المنوفية، 1437/ 2016.
22. د. شريف درويش اللبان، تكنولوجيا الإتصال، المخاطر والتحديات والتأثيرات الاجتماعية، سلسلة العلوم والتكنولوجيا، الدار المصرية اللبنانية، 2008.
23. د. صالح محمد بدر الدين، المسئولية عن نقل النفايات الخطرة في القانون الدولي، دار النهضة العربية، 2005.
24. د.صفات أمين سلامة، وخليل قورة، تحديات عصر الروبوتات وأخلاقياته، مركز الإمارات للدراسات والبحوث الإستراتيجية، 2012.
25. ا. د. صلاح الدين عامر، مقدمة لدراسة القانون الدولي العام، دار النهضة العربية، الطبعة الثانية، 2007.
26. د.عامر الزمالي، آليات تنفيذ القانون الدولي الإنساني، دراسات في القانون الدولي الإنساني، دليل للتطبيق علي الصعيد الوطني، إعداد نخبة من المتخصصين، تقديم أ.د.أحمد فتحي سرور، دار المستقبل العربي، 2003.
27. د. عثمان عبد اللطيف، الألغام الأرضية والمسئولية الدولية بين القانون الدولي العام والشريعة الإسلامية، والألغام الأرضية في الأراضي المصرية نموذجا، دراسة مقارنة، الطبعة الأولي، دار النهضة العربية، 2015.
28. د. عبد الحميد بسيوني، الذكاء الاصطناعي والوكيل الذكي، دار الكتب العلمية للنشر والتوزيع، 2005.
29. د.عبد الشافي عبد الدايم، الشركات الأمنية الخاصة في ظل القانون الدولي الإنساني، المجلة المصرية للقانون الدولي، المجلد الثاني والسبعون، عام 2016.
30. د. عبد الغني محمود، القانون الدولي الإنساني- دراسة مقارنة بالشريعة الإسلامية، الطبعة الأولي، دار النهضة العربية، 1991.
31. د.عبد الوهاب أحمد عبد الوهاب بدر، أسلحة الدمار الشامل في ضوء قواعد القانون الدولي العام، "دراسة تطبيقية على الشرق الأوسط" دار الجامعة الجديدة، 2018.

32. د.عبد علي سوادي، المسئولية الدولية عن انتهاك قواعد القانون الدولي الإنساني، المركز العربي للدراسات والبحوث العلية للنشر والتوزيع، 1438-2017.
33. د. عصام زناتي, المسئولية الدولية عن الأضرار الناجمة عن الأجسام الفضائية، دار النهضة العربية، 2003/2002.
34. د. علي محمد خلف، المسئولية عن الأشياء غير الحية الناتجة عن الخطأ المفترض- مسئولية المنتج البينية نموذجا " دراسة مقارنة" مجلة المحقق الحلي للعلوم القانونية و السياسية، العدد الثاني، السنة السابعة، 2015.
35. د. فاطمه جلال عبدالله، تطور المسئولية المدنية للجراح عن الجراحات الحديثة " الجراحات الروبوتية " أعمال مؤتمر القانون والتكنولوجيا المنعقد في الفترة من التاسع إلي الحادي عشر من شهر ديسمبر2017، كلية الحقوق- جامعة عين شمس.
36. فريتس كالسهوفن، الاتفاقية الخاصة بالاسلحة التقليدية " المباديء القانونية التي بنيت عليها الاتفاقية " المجلة الدولية للصليب الاحمر، السنة الثالثة، نوفمبر/ ديسمبر، العدد السادس عشر، 1990.
37. ماركوساسولي، الأسلحة ذاتية التشغيل والقانون الدولي الإنساني: مزايا وأسئلة تقنية مطروحة ومسائل قانونية يجب توضيحها - بحث منشور ضمن إصدار اللجنة الدولية للصليب الأحمر بالقاهرة " القانون الدولي الإنساني في النزاعات المسلحة المعاصرة " 2017.
38. د. محمد حافظ غانم، المسؤولية الدولية- دراسة لأحكام القانون الدولي و لتطبيقاتها التي تهم الدول العربية، معهد الدراسات العربية العالمية-جامعة الدول العربية، 1962.
39. د.محمد حافظ غانم، الوجيز في القانون الدولي العام، دار النهضة العربية، 1979.
40. د. محمد صافي، القانون الدولي العام، دار النهضة العربية، 2019.
41. د. محمد عبد الصمد مهنا، المحكمة اللبنانية الدولية الخاصة، المجلة المصرية للقانون الدولي، العدد التاسع و الستون، عام 2013، ص535، و انظر أيضا: د. أحمد ابو الوفا، الملامح الأساسية للنظام الأساسي للمحكمة الجنائية الدولية، المجلة المصرية للقانون الدولي، العدد الثامن والخمسون، عام 2002.
42. د.محمد عبد الكريم عزيز، مسئولية المقاتل عن انتهاك القانون الدولي الإنساني، الطبعة الأولي، مركز الدراسات العربية، 2017.
43. أ. د. محمد لبيب شنب، نظرة في مسؤولية الأطباء عن الاشياء التي في حراستهم، مجلة المحامي- جمعية المحامين الكويتية، العدد السابع و الثامن و التاسع، يناير- فبراير- مارس 1981.

44. د.مصطفي فؤاد، القانون الدولي الإنساني، دار المطبوعات الجامعية، 2019.
45. د. مصطفى أحمد فؤاد، النظام القانوني الدولي، دار المطبوعات الجامعية، 2019.
46. د. محمد سعادي، أثر التكنولوجيا المستحدثة على القانون الدولي العام، دار الجامعة الجديدة، 2014.
47. نجوي محمد عبد الرحمن عثمان، تعويض الأضرار الناشئة عن جرائم الإرهاب " دراسة مقارنة"، رسالة ماجستير، كلية الحقوق - جامعة المنوفية، 2017.
48. د.هشام عمر أحمد الشافعي، المسئولية الدولية عن الأضرار الناجمة عن الأنشطة الفضائية النووية، شركة الدليل للدراسات و التدريب و أعمال الطباعة والنشر، 2013.
49. هورتنسيا دي . تي. جوتيريس بوسي، العلاقة بين القانون الدولي الإنساني و المحاكم الجنائية الدولية، مختارات من المجلة الدولية للصليب الأحمر، 2006.
50. د.هشام عمر أحمد الشافعي، المسئولية الدولية عن الأضرار الناجمة عن الأنشطة الفضائية النووية، شركة الدليل للدراسات والتدريب وأعمال الطباعة والنشر، 2013.
51. ليزانوكس، قصة تكنولوجيا الروبوتات، الدار العربية للعلوم، ناشرون، 2012.
52. الاسلحة ذاتية التشغيل - ضرورة اتفاق الدول علي معني السيطرة البشرية فعليا، اللجنة الدولية للصليب الأحمر. منشور علي :
https://www.icrc.org/ar/autonomous-weapons-states-must-agree-what-human-control-means-practice ,
53. ناثالي جوبيرت، شبح الروبوتات القاتلة - استخدام الطائرات بدون طيار في الميدان، 18 حزيران (يونيو) 2013 الساعة 5:48 مساءً - تم التحديث بتاريخ 19 حزيران (يونيو) 2013 الساعة 7:42 مساءً متاح علي:
54. http: //robots.blog.lemonde.fr تاريخ الاطلاع: 31 ديسمبر 2020، الساعة4م.
55. قرار البرلمان الأوروبي المؤرخ في الثاني عشر من سبتمبر2018 بشأن أنظمة الأسلحة، : متاح علي :
http://www.europarl.europa.eu/sides/getDoc.do?pubRef=//EP//NONSGML+TA+P8-Ta-2018-0341+0+DOC+PDF+V0//FR.

- مراجع أجنبية:

1. A/HRC/23/47
2. Ccw/GGE.1/20/2017/3
3. CCW/MSP/2015/3.
4. CCW/CONF.V/2 .
5. A/65/321 para36 .
6. Brownies, Principles of Public international law, (8th Edition), Edited by: James Crawford, Oxford University Press, 2012,
7. Danial N. Hammond, Autononomous Weapons and the Problem of Ststе Accountability, Chicugho Journal of International law, volume 15, number 2, Article 8, 2015 .
8. Final report of defense Defense science board, U.S. Department of Defense, Task Force Re-Port: The Role of Autonomy in (DOD) systems, 1, 21 (July 2012.
9. Final Report of the Defense Science Board (DSB) Task Force on: the Role of Autonomy in Department of Defense (DoD) Systems, Chairman, DSB: Dr. Paul Kaminski, Department of Defense, Defense Science Board, (July 2012). Hin Yan Liu, Gorization and legality of autonomous remote weapons system, international review of the Red cross, volume 94, No: 886, summer 2012,
10. Karen Parker, Memorandum on weapons and the laws and customs of war, Intrnational Educational Development, Humanitarian Law Project, May 1997.
11. Ian GR Shaw, Robot Wars: US Empir and geopolitics in the robotic age, article in security dialogue, vol. 48(5), 2017.
12. Jonathan Crowe and Kylie Weston – Scheuber, Principles of International Humanitarian Law, Edward Elgar publishing Limited, 2013.
13. Judith A. Markowitz, roborts that kill: deadly machines and their precursors in myth ,Folklore, Literature, Popular Culture and Reality, Publisher: Mcfarland Company (April 11, 2019) .
14. Marc Cannellos and Rachel Haga, Lost in translation building a common language for regulating autonomous weapons, Published in IEEE Technology and Socitry Magazine, September 2016.
15. Michael N. Schmitt & Jeffrey S. Thurnher, “Out of the Loop”: Autonomous Weapon Systems and the Law of Armed Conflict, Harvard National Security Journal (2013), 231, 242–43.
16. Nehal Bhuta, Antonino Rotolo and Giovanni Sartor, Awareness and Responsibility in Autonomous Weapons Systems, Department of Law, European University Institute, Florence, Italy, CIRSFID and Department of Legal Studies, University of Bologna, Italy, 2019.
17. Nicholas tsagourias and Alasdair Morrison, international humanitarian law, Cases, Materials and Commentary, Cambridge University Press, Online publication date: August 2018,
18. Ugo Pagallo, the laws of robots: crimes, contracts and torts, law, governance and technology series, volume 10, 2013, Series Editors: Pompeu Casanovas and Giovanni Sartor, Springer Science+Business Media Dordrecht 2013.
19. CCW/MSP/2015/3
20. E/CN.4/2005/7
21. A/61/311
22. A/HRC/14/14/Add.6 .

جرائم الإرهاب السيبراني باستخدام الطائرات المسيرة (Drones)

التحديات الأمنية واستراتيجية المواجهة

بقلم

الدكتور/ عماد الدين محمد كامل عبد الحميد

أستاذ القانون الجنائي المساعد

كلية الإمام مالك للشريعة والقانون – دبي

مجلة علمية محكمة | العدد (15) | السنة العاشرة | ذو القعدة 1443 هـ | يونيو 2022م

جرائم الإرهاب السيبراني باستخدام الطائرات المسيرة (Drones)

التحديات الأمنية واستراتيجية المواجهة

د/ عماد الدين محمد كامل عبد الحميد

أستاذ القانون الجنائي المساعد - كلية الإمام مالك للشريعة والقانون - دبي

مقدمة عامة

أصبحت البنى التحتية لمرافق الأمن القومي في مختلف دول العالم المتقدم مدرجة عبر الفضاء السيبراني، القائم على تكنولوجيا تقنية المعلومات وتقنية الاتصالات، بما تتضمنه مرافق تلك البنى من أنشطة ومعلومات وأسرار وبيانات، في جميع النواحي والمجالات الصناعية منها والاقتصادية، العسكرية منها والطاقة والمياه والصحة ومنظومة النقل وقطاع البنوك ومختلف المؤسسات المالية والحكومية، لذا فقد أحاطت تلك المعلومات والبيانات والأسرار بسياج منيع من الحماية المادية والتقنية وأجهزة المراقبة التكنولوجية وعبر برامج حماية أو بتشفير لمنع الوصول إليها أو فك شفراتها، فضلاً عما تضمنه ذلك الفضاء السيبراني من معلومات لأفراد الدول وتعاملاتهم في جميع نواحي الحياة، فأصبح ذلك العالم بمؤسساته ومرافقه، بدوله وأفراده وجماعاته أسيراً لذلك الفضاء السيبراني الذي صنعه الإنسان لنفسه، لا يملك منه فكاكاً، رهينة تحت تصرفه يحترم قواعده ويُصغي لآلياته ويناقش فرضياته[1]، وأول هذه الفرضيات أن أصبح الفضاء السيبراني بمكوناته السابقة قوة جذب للاعتداء عليه سواء من قبل الأفراد بارتكاب جرائم تقنية المعلومات، أو من قبل المنظمات الإرهابية وهو ما يُعرف بالإرهاب السيبراني، أو من قبل الدول وأجهزتها الاستخباراتية والعسكرية وهو ما يُعرف بالحروب السيبرانية والحروب الإلكترونية، لكونه هدفاً سهلاً وآمناً وغير مكلفٍ وناجحاً في تحقيق أهداف المعتدي وفي ثوان معدودة ودون ضبط أو ملاحقة للمعتدي. وثاني هذه الفرضيات هي تلك التطبيقات الذكية والتي تُعد الطائرات بدون طيار ويُطلق عليها الطائرات المسيرة أهم وأخطر تلك التطبيقات، وأهم وأخطر الوسائل لتنفيذ الهجمات السيبرانية، سواء اتخذت تلك الهجمات صورة جرائم سيبرانية تقليدية أو جرائم الإرهاب السيبراني أو الحروب السيبرانية أو حروب إلكترونية، فقد بدأ استخدام الطائرات المسيرة في الأنشطة الترفيهية ثم سرعان ما تطورت تقنية صناعتها فأصبحت مزودة بكاميرات عالية الدقة، وأجهزة استشعار عن بُعد، وأجهزة مراقبة دقيقة ومسح بيانات ومواقع، وأجهزة رسم خرائط ثلاثية الأبعاد، وتزويدها ببرمجيات خاصة تستطيع أن تنفذ كل المهام المطلوبة منها على اختلاف أنواعها ودقتها وإرسال التقارير والبيانات المطلوبة في ثوان معدودة للمستخدم، فضلاً عن صغر حجم تلك الطائرات، وعدم قدرة أجهزة وأنظمة الرصد التقليدية على رصدها، وعدم القدرة على ضبط وملاحقة مستخدمها الذي قد يبعد عنها بالكيلو مترات، الأمر الذي ترتب عليه أن أصبحت أداة جوهرية لتنفيذ الهجمات السيبرانية بصورها السابقة (جرائم سيبرانية تقليدية أو جرائم الإرهاب السيبراني أو الحروب السيبرانية أو حروب إلكترونية)، كما أن تزايد استخدام تلك الطائرات بين دول العالم في جميع المجالات الحيوية والاستراتيجية جعلها تحتل مكانة مهمة لدى مؤسسات ومرافق الأمن القومي للدول لاستخدامها في دعم الأنشطة والممارسات المتعلقة بسلطاتها واختصاصاتها، الأمر الذي جعلها هدفاً لأي هجوم سيبراني لما تحتويه تلك الطائرات من معلومات وبيانات حساسة والتي قد تكون مرتبطة بمراكز القيادة والتحكم داخل مؤسسات ومرافق الأمن القومي للدول، ومن ثم أصبح وجود أي تهديد أو هجوم سيبراني على تلك الطائرات يُعد تهديداً أو هجوماً على الأمن القومي السيبراني للدول.

لذا فلم يُعد مفهوم الأمن القومي لمختلف دول العالم المتقدم قاصراً على تلك النواحي التقليدية العسكرية والأمنية، بل اتسع ذلك المفهوم وتطور لكي يتناسب مع حجم التحديات والتهديدات والمخاطر والأضرار التي ترتبت على إدراج مرافقه ومؤسساته في جميع النواحي والمجالات عبر ذلك الفضاء السيبراني، وما تتضمنه من أسرار ومعلومات وبيانات تتسم بالطابع الفني التقني يتم تداولها ومعالجتها والتعامل معها عبر تقنيات وآليات وفرضيات وتهديدات ذلك الفضاء السيبراني. فقد فرض واقع الحروب السيبرانية والإرهاب السيبراني وهجماتهم على البنى التحتية للدول خاصة باستخدام الطائرات المسيرة ضرورة وجود منظومة قوية ومتطورة للأمن السيبراني لتأمين وحماية

(1) د. عماد الدين محمد كامل عبد الحميد،" استراتيجية تعزيز الأمن السيبراني للاقتصاد الرقمي- دراسة في العملات الرقمية للبنوك المركزية (CBDC))، مجلة الاقتصاد الإسلامي، دبي، الجزء الأول العدد 485، مارس 2021، ص 23، الجزء الثاني العدد 486، إبريل 2021 ص 25. - رابط الجزء الأول ورابط الجزء الثاني:
Els485.pdf/03/https://www.aliqtisadalislami.net/wp-content/uploads/2021
Els486.pdf/04/https://www.aliqtisadalislami.net/wp-content/uploads/2021

تلك البنى التحتية والتي تُشكل مفردات الأمن القومي لها، فضعف منظومة الأمن السيبراني أصبح وبحق يهدد الأمن القومي للدول، لذا فقد ارتبط الأمن السيبراني بالأمن القومي وتصدَر الأمن السيبراني على لائحة أولويات الأمن القومي للدول، ناهيك عن استخدام تلك الطائرات المسيرة في عمليات التجسس والقرصنة والتهريب والعمليات الإرهابية الأخرى.

الأمر الذي تطلب استقراء لاستراتيجيات تحقيق الأمن السيبراني لمرافق الأمن القومي سواء تلك التي تم وضعها من قبل خبراء الأمن السيبراني أو تلك الاستراتيجيات التي وضعتها الدول لتحقيق الأمن السيبراني لمواجهة الإرهاب السيبراني، وذلك لتقييمها والوقوف على مدى قدرتها على مكافحة الإرهاب السيبراني باستخدام الطائرات المسيرة، حتى يتمكن الباحث من بيان رؤيته ووضع استراتيجيته، لذا سوف تُجسد مفردات موضوع البحث وخطته معالجة كل ما سبق ذكره.

مشكلة البحث:

تتجسد في مجموعة من الإشكاليات القانونية والفنية والأمنية تتمثل في:

- المخاطر والتحديات التي يفرضها الإرهاب السيبراني وتقنياته المتطورة المُرتكبة ضد مرافق البنى التحتية للدول والتي تُجسد مرافق ومؤسسات الأمن القومي، مع إشكالية تزايد وتيرة الهجمات السيبرانية وتطور تقنياتها وصعوبة تحديد مصدرها.
- إشكالية ضعف منظومة الأمن السيبراني لأغلب دول العالم.
- إشكالية وضع الحد الفاصل بين ما يُعد إرهاباً سيبرانياً وما يُدخل في مفهوم الحروب السيبرانية، خاصة أن هناك قاسماً مشتركاً بينهما يتمثل في الهجوم السيبراني ومحل الاعتداء وهو مرافق البنى التحتية، وإشكالية الجدل القانوني حول نوع الحماية المطلوبة.
- الإشكاليات القانونية والفنية والأمنية التي تفرضها الطائرات المسيرة مع تطور تقنية صناعتها وخصائصها الفريدة، فأصبحت أحدث وسائل ارتكاب الإرهاب السيبراني للاعتداء على مرافق الأمن القومي.
- إشكالية استخدام الطائرات المسيرة في عمليات التجسس والقرصنة والتهريب.
- إشكالية أن تلك الطائرات هدفاً للهجمات السيبرانية لما تتضمنه من بيانات حساسة وأسرار، وما يُثيره كل ذلك من إشكاليات قانونية تتعلق بصعوبة ضبط تلك الجرائم وملاحقة مرتكبيها، وإيجاد تنظيم قانوني قوي، ومنظومة للأمن السيبراني قوية ومتطورة.

نطاق موضوع البحث:

يقتصر على الإرهاب السيبراني باستخدام الطائرات المسيرة ذات الاستخدام المدني وما تُثيره من تحديات قانونية وأمنية وما تتطلبه من وضع استراتيجية لمواجهة تلك التحديات.

أهمية موضوع البحث:

تتجسد في بيان:

- مفهوم الإرهاب السيبراني ومظاهره الحديثة المتطورة، وبيان مفهوم الحروب السيبرانية والحروب الإلكترونية، وأسباب تحول الإرهاب وحروب الدول إلى الفضاء السيبراني، وأسباب تزايد وتيرة الهجمات السيبرانية على مرافق البنى التحية لمختلف الدول، وفض الاشتباك والتداخل بين ما يُعد إرهاباً سيبرانياً وما يُعد حرباً سيبرانية.
- التحديات القانونية والأمنية التي يفرضها الإرهاب السيبراني على مرافق البنى التحتية لمرافق الأمن القومي للدول، ومدى ارتباط ذلك بمنظومة الأمن السيبراني للدول ومؤشر الأمن السيبراني العالمي، وبيان هجمات الإرهاب السيبراني على مرافق الأمن القومي للدول 2020-2021.
- ماهية الطائرات المسيرة من حيث بيان تعريفها والبنى التحتية الخاصة بها، وأنواعها وتعدد وتنوع استخداماتها، والتنظيم القانوني للطائرات المسيرة في دولة الإمارات العربية المتحدة.
- الهجوم السيبراني باستخدام الطائرات المسيرة وتهديدات الأمن القومي، واستخدامها في عمليات التجسس والقرصنة والتهريب والعمليات الإرهابية، والهجوم السيبراني الواقع على الطائرات المسيرة ومظاهره.
- استراتيجية تحقيق الأمن السيبراني لمرافق الأمن القومي، من خلال استخدام تقنية البلوكشين، والاستراتيجيات التي وضعتها كل دولة، واستراتيجية صندوق النقد الدولي التي وضعها لحماية الأمن السيبراني للقطاع المالي للدول، واستراتيجية الباحث لتحقيق الأمن السيبراني لمواجهة الإرهاب السيبراني.

الدراسات السابقة:

لا توجد دراسات سابقة تتعلق بموضوع الإرهاب السيبراني باستخدام الطائرات المسيرة، وكل الدراسات الموجودة تنفرد بالإرهاب السيبراني ومظاهره ودون وضع استراتيجية مواجهة، أو تتعلق بالطائرات المسيرة ومدى تقرير المسؤولية المدنية، أو دراسة إشكالياتها التي تتعلق بالقانون الدولي الإنساني، ودون تناول موضوع الإرهاب السيبراني باستخدام تلك الطائرات.

أهداف البحث:

هو حل إشكالياته من خلال مواجهة تلك التحديات القانونية والأمنية للإرهاب السيبراني باستخدام الطائرات المسيرة، وذلك بوضع استراتيجيات لتحقيق الأمن السيبراني لمواجهة الإرهاب السيبراني، فضلاً عن استراتيجية وضعها الباحث لتحقيق الأمن السيبراني لمواجهة تحدياته.

منهجية البحث:

هو المنهج الاستقرائي والمنهج التحليلي المقارن، المنهج الاستقرائي من خلال استقراء حقيقة وجوهر الإرهاب السيبراني وبيان مظاهره وجوهر وخصائص الطائرات المسيرة وارتباطها بالإرهاب السيبراني، للوصول إلى حجم الأضرار الواقعة على مرافق الأمن القومي، واستقراء لاستراتيجيات تحقيق الأمن السيبراني لمرافق الأمن القومي سواء تلك التي تم وضعها من قبل خبراء الأمن السيبراني أو تلك الاستراتيجيات التي وضعتها الدول لتحقيق الأمن السيبراني لمواجهة الإرهاب السيبراني، وذلك لتقييمها والوقوف على مدى قدرتها على مكافحة الإرهاب السيبراني باستخدام الطائرات المسيرة، حتى يتمكن الباحث من بيان رؤيته ووضع استراتيجيته، والمنهج التحليلي المقارن، من خلال تحليل التحديات القانونية والأمنية التي يفرضها الإرهاب السيبراني باستخدام الطائرات المسيرة، بهدف وضع استراتيجيات المواجهة.

خطة البحث:

تم تقسيمه إلى ثلاثة مباحث ولكل مبحث مطلبين، المبحث الأول ماهية الإرهاب السيبراني، المطلب الأول مفهوم الإرهاب السيبراني وبيان مظاهره، المطلب الثاني الإرهاب السيبراني وتحديات الأمن القومي للدول، المبحث الثاني الإرهاب السيبراني المرتبط بالطائرات المسيرة، المطلب الأول ماهية الطائرات المسيرة (Drones)، المطلب الثاني الهجوم السيبراني باستخدام الطائرات المسيرة وتهديدات الأمن القومي، المبحث الثالث استراتيجية تحقيق الأمن السيبراني لمرافق الأمن القومي، المطلب الأول محاور استراتيجية تحقيق الأمن السيبراني لمرافق الأمن القومي المطلب الثاني استراتيجيات الدول لتحقيق الأمن السيبراني لمواجهة الإرهاب السيبراني.

المبحث الأول
ماهية الإرهاب السيبراني

تمهيد:

سوف نتناول دراسته من خلال مطلبين، المطلب الأول مفهوم الإرهاب السيبراني وبيان مظاهره، بدراسة أسباب تحول الإرهاب وحروب الدول إلى الفضاء السيبراني، وبيان مفهومه ومظاهره وأشهر الهجمات السيبرانية 2020 (هجوم Solar Winds)، والمطلب الثاني الإرهاب السيبراني وتحديات الأمن القومي للدول، ببيان تطور مفهوم الأمن القومي ومدى ارتباطه بالأمن السيبراني، تعريف الأمن السيبراني، هجماته على مرافق الأمن القومي للدول 2020 2021-، على النحو التالي:

المطلب الأول: مفهوم الإرهاب السيبراني وبيان مظاهره
المطلب الثاني: الإرهاب السيبراني وتحديات الأمن القومي للدول

المطلب الأول

مفهوم الإرهاب السيبراني وبيان مظاهره

تمهيد:

سوف نتناول دراسته من خلال عدة محاور، وذلك على النحو التالي:

المحور الأول
أسباب تحول الإرهاب وحروب الدول إلى الفضاء السيبراني:

أولاً:أسباب قوة جذب الفضاء السيبراني للمنظمات الإرهابية:

فالفضاء السيبراني أصبح قوة جذب للاعتداء عليه من قبل المنظمات الإرهابية، للأسباب التالية:

- إدراج مختلف دول العالم مؤسسات ومرافق البنى التحتية عبر الفضاء السيبراني، ومن ثم أصبحت هدفاً محدداً للاعتداء عليها.
- صعوبة تحديد مصدر تلك الهجمات الإرهابية السيبرانية وتعقبها، ومن ثم ضبط مرتكبيها وملاحقتهم.
- إن الهجمات الإرهابية السيبرانية عابرة للحدود حول العالم، فيتم تنفيذها دون الحاجة إلى السفر ومخاطره وتكاليفه وإعدادات العملية الإرهابية.
- الوقت الذي تستغرقه تلك المنظمات الإرهابية لاستغلال ثغرة أمنية بعد اكتشافها قصير نسبيًا، ومن ثم تستطيع تحقيق أهدافها بسهولة ودون وجود ردود أفعال قوية تجاهها أو مشاكل عند التنفيذ، عكس تنفيذ تلك المنظمات لهجماتها التقليدية خارج الفضاء السيبراني.
- إن تكنولوجيا الهجوم السيبراني وتقنياته أصبحت متاحة على نطاق واسع ورخيصة نسبيًا، مقارنة بأساليب الإرهاب التقليدية الأخرى.
- إن أساليب الهجوم السيبراني وتقنياته يمكن استخدامها في إصابة هدف واحد مرات متكررة، أو إصابة أهداف متعددة في وقت واحد وفي ثوان معدودة، عكس أسلحة الإرهاب التقليدية فلا يمكن استخدامها إلا مرة واحدة.

ثانياً: أسباب قوة جذب الفضاء السيبراني لحروب الدول (الحرب السيبرانية):

- أن الآثار المدمرة للهجوم السيبراني في الحروب السيبرانية على أحد مراكز البنى التحتية لدولة معينة تفوق قدراتها بمراحل الآثار المدمرة للهجوم العسكري التقليدي، وصعوبة

تحديد مصدر الهجوم ومن ثم تحديد الدولة المعتدى ومحاسبتها من جانب الدولة المعتدي عليها أو من المجتمع الدولي.

- صعوبة اكتشاف ارتكاب الهجوم السيبراني في الحروب السيبرانية، أو تحديد حجم الأضرار التي ترتبت عليه، فقد يتم الهجوم وينتهي دون حتى اكتشافه، أو اكتشاف حجم ونوعية الأسرار التي تم الاستيلاء عليها، ودون وجود أي دليل مادي أو حتى تقني على تحديد هوية المعتدي.
- الهجوم السيبراني في الحروب السيبرانية عابر للحدود الدولية وآلية للتدمير عن بُعد، يوفر للدولة المعتدية الوقت والمال والجهد، ويُجنبها أي خسائر في الأموال أو المعدات العسكرية أو الأرواح، فبمجرد اكتشاف الثغرة الأمنية على الطرف الآخر من الكرة الأرضية يبدأ وينتهي في ثوان معدودة.
- قد يكون هدف الحروب السيبرانية هو زعزعة الأمن والاستقرار داخل الدولة المعتدي عليها أو إشاعة الفوضى لقلب أو تغيير نظام الحكم فيها لصالح طرف، وهو ذات هدف ووسيلة المنظمات الإرهابية في الإرهاب السيبراني، وهو التهديد والترويع وإشاعة الذعر لدى الدولة المعتدى عليها وأجهزتها ومؤسساتها وأفرادها لإرغامها على القيام بعمل أو الامتناع عن عمل، بإصابة مرفق حيوي.

المحور الثاني
مفهوم الإرهاب السيبراني – الحروب السيبرانية- الحروب الإلكترونية:

الجدير بالذكر أن هناك حقيقة مهمة لا بد وأن نشير إليها، وهي أنه لا يوجد اتفاق عالمي سواء في مجال الفقه أو لدى المؤسسات الرسمية حول تعريف العديد من الأنشطة الإجرامية المرتبطة بالإنترنت مثل الإرهاب السيبراني والحرب السيبرانية والحرب الإلكترونية والجريمة الإلكترونية.

أولاً:تعريف الإرهاب السيبراني:

عرفه Jonalan Brickey جونالان بريكي بأنه "استخدام القدرات السيبرانية لإجراء وتمكين العمليات المسلحة التخريبية والمدمرة في الفضاء الإلكتروني، لخلق واستغلال الخوف من خلال العنف أو التهديد بالعنف سعياً وراء التغيير السياسي"[1]، ويُعرِّف (William L. Tafoya) ويليام تافويا في نشرة إنفاذ القانون التابعة لمكتب التحقيقات الفيدرالي الإرهاب السيبراني بأنه "تخويف المؤسسة المدنية من خلال استخدام التكنولوجيا المتقدمة لتحقيق أهداف سياسية أو دينية أو

(1) Jonalan Brickey , 'Defining Cyberterrorism: Capturing a Broad Range of Activities in Cyberspace', CTC Sentinel, August 2012, Vol. 5, No. 8, p. 6. https://ctc.usma.edu/wp-content/uploads/2012/08/CTCSentinel-Vol5Iss81.pdf

أيديولوجية، وهي الإجراءات التي تؤدي إلى تعطيل أو حذف بيانات أو معلومات البنية التحتية المهمة[1]، وقدم Kelly A. Gable كيلي جابل تعريفًا مشابهًا، بما في ذلك "جهود الإرهابيين لاستخدام الإنترنت لاختطاف أنظمة الكمبيوتر، أو إسقاط النظام المالي الدولي [2]، وعرفته سوزان برينر Susan W. Brenner خبيرة الأمن السيبراني، بأنه استخدام تكنولوجيا الكمبيوتر للانخراط في نشاط إرهابي[3]، كما تُعرفه دورثي دينينغ (Dorothy Denning) بأنه "هجوم قائم على الحاسوب، ومشابه للأفعال المادية للإرهاب يهدف إلى الترويع أو الإجبار للحكومات أو للمجتمعات لتحقيق أغراض سياسية أو دينية أو عقائدية، ويكون مدمرًا وتخريبيًّا لتوليد الخوف"[4].

ومن أشهر التعريفات الحديثة قبولاً للإرهاب السيبراني "هو قتل أو إيذاء غير المقاتلين الأبرياء العزل، أو تدمير البنية التحتية الحيوية التي يتم التحكم فيها عبر الإنترنت لإحداث ضرر مادي، من خلال وسائل الهجمات الإلكترونية أو العمليات الإلكترونية من قبل جهات فاعلة حكومية أو غير حكومية أو فردية بقصد إثارة الخوف من أجل تعزيز غايات سياسية أو دينية أو أيديولوجية"[5].

وفي مجال تعريف المؤسسات الدولية الرسمية للإرهاب السيبراني يُعرِّفه المركز الوطني الأمريكي لحماية البنية التحتية بأنه "عمل إجرامي يُرتكب من خلال أجهزة الكمبيوتر مما يؤدي إلى العنف أو الموت أو التدمير، وخلق الرعب بغرض إجبار الحكومة على تغيير سياساتها[6]، ومركز الدراسات الاستراتيجية والدولية واشنطن (CSIS)بأنه "استخدام لأدوات شبكة الكمبيوتر من أجل إغلاق البنى التحتية الحيوية الوطنية (كالطاقة والنقل والعمليات الحكومية) أو لإكراه أو ترهيب الحكومة أو السكان المدنيين[7]، وتُعرِّف استراتيجية الأمن السيبراني في النمسا لعام 2013 الإرهاب السيبراني

(1) William L. Tafoya, Ph.D., Cyber Terror, FBI Law Enforcement Bulletin, Nov. 2011, https://www.fbi.gov/stats-services/publications/law -enforcement-bulletin/November- 2011/cyber-terror. file:///C:/Users/alfat/Downloads/november-2011-leb.pdf

(2) Kelly A. Gable, Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent, 43 Vand. J. Transnat'l L. 57, 62 (2010).

(3) Susan W. Brenner, "At Light Speed" - Attribution and Response to Cybercrime/Terrorism/Warfare, 97 J. Crim. L. & Criminology 397, 386 (2007) (categorizing cyber-threats and focusing on attribution as the key element to be solved in battling those threats).

(4) Denning, Dorothy, E," Cyber terrorism"، Global Dialogue, Aug 2000, p01.

(5) Christopher O'Brien," What is cyber-terrorism, and is it a threat to U.S. national security?" Small wars journal, Thu, 11/04/2021. https://smallwarsjournal.com/jrnl/art/what-cyber-terrorism-and-it-threat-us-national-security#_edn12

(6) Clay Wilson, Cong. Research Serv., RL32114, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress 4 (2003) (Quoting Ron Dick, then Director of the NIPC).

(7) James A. Lewis," Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats, Center for Strategic and International Studies, December 2002. https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/021101_risks_of_cyberterror.pdf

على أنه "جريمة ذات دوافع سياسية ترتكبها جهات فاعلة حكومية أو غير حكومية"[1]، وتقرير الدفاع السيبراني والأمن السيبراني الوطني لليابان في سبتمبر 2020 بأنه "أي هجمات تستخدم شبكات المعلومات والاتصالات وأنظمة المعلومات التي يمكن أن يكون لها تأثير كبير على حياة الناس والأنشطة الاجتماعية والاقتصادية"[2].

ثانياً: تعريف الحروب السيبرانية:

الحروب السيبرانية[3] هي " أنشطة الهدف منها تحقيق التفوق المعلوماتي من أجل الإضرار أو التهديد لأنظمة المعلومات وما تتضمنه من أسرار أو معلومات تتعلق بجميع النواحي العسكرية أو الاقتصادية أو السياسية "[4]، أو مهاجمة نظم المعلومات لدولة أخرى أو إبطاء خدماتها أو إضرارها أو الاستيلاء عليها [5]، أو هي الهجمات الرقمية من قبل دولة على مرافق البنى التحتية لدولة أخرى، من خلال فيروسات الكمبيوتر وعمليات القرصنة لتعطيل أنظمة الكمبيوتر الحيوية لتلك الدولة، لإحداث أضرار في الأنفس أو الأرواح [6] أو هي أعمال تقوم بها دولة ضد دولة أخرى من أجل اختراق أجهزة الكمبيوتر والشبكات التابعة لتلك الدولة لتعطيلها أو لحقيق أضرار بالغة[7].

(1) Stefan Soesanto, "Cyber Terrorism. Why it exists, why it doesn't, and why it will", ARI 472020/ - 172020/4/. http://www.realinstitutoelcano.org/wps/portal/rielcano_en/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_in/zonas_in/ari47-2020-soesanto-cyber-terrorism-why-it-exists-why-it-doesnt-and-why-it-will

(2) CYBERDEFENSE REPORT, Japan's National Cybersecurity and Defense Posture, Policy and Organizations, Zürich, September 2020, Cyber Defense Project (CDP) Center for Security Studies (CSS)، ETH Zürich https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2020-08-Japans-national-cybersecurity-defense-posture.pdf

(3) د. عماد الدين محمد كامل عبد الحميد،" استراتيجية تعزيز الأمن السيبراني للاقتصاد الرقمي - دراسة في العملات الرقمية للبنوك المركزية (CBDC)"، مجلة الاقتصاد الإسلامي، دبي، الجزء الثاني العدد 486، إبريل 2021 ص 25. https://www.aliqtisadalislami.Els486.pdf/04/net/wp-content/uploads/2021

(4) UNTERM, "Cyber warfare" warfare, https://unterm.un.org/UNTERM/display/Record/UNHQ/NA/c263537. View at: Google Scholar

(5) S. Sagiroglu, "Cyber security and defence: importance, definitions and precautions," in Cyber Security and Defence—Awareness and Deterrence, vol. 1, pp. 21–45, Grafiker Press, Ankara, Turkey, 2018.View at: Google Scholar

(6) Steve Ranger," What is cyberwar? Everything you need to know about the frightening future of digital conflict", December 4, 2018. https://www.zdnet.com/article/cyberwar-a-guide-to-the-frightening-future-of-online-conflict/

(7) Richard A. Clarke & Robert knake, Cyber War: The Next Threat to National Security and What to Do About It, HarperCollins, 2010, p:6.

ثالثاً: تعريف الحروب الإلكترونية:

الحرب الإلكترونية كما حددتها وزارة الدفاع الأمريكية هي الأنشطة العسكرية التي تستخدم الطاقة الكهرومغناطيسية للتحكم في الطيف الكهرومغناطيسي (نطاق الترددات الكهرومغناطيسية) أو مهاجمة العدو [1]، فتدعم الحرب الإلكترونية القيادة والسيطرة بالسماح للقادة العسكريين بالوصول إلى نطاق الترددات الكهرومغناطيسية للتواصل مع القوات، مع منع الخصوم المحتملين من الوصول إليها لتطوير العمليات والتواصل مع القوات.

المحور الثالث
تداخل مفهوم الإرهاب السيبراني والحروب السيبرانية:

وأسباب ذلك تتجسد في الخصائص المشتركة التي تجمع بينهما أولها أن محل ارتكابهما عبر ذلك الفضاء السيبراني وثاني تلك الخصائص أن وسائل ارتكابهما يكون باستخدام الهجوم الإلكتروني، وثالث تلك الخصائص أن الهدف من ارتكابهما مشترك، وإن وردت بعض التعريفات بشأن الحروب السيبرانية تتضمن أن مرتكبي تلك الحروب السيبرانية هي دولة ضد دولة أخرى ومن ثم حاولت وضع حد فاصل يميز بينهما، إلا أن تلك المحاولات لم تنجح في فض الاشتباك بينهما، فما زالت هناك تعريفات تؤكد ذلك التداخل مثل تعريف استراتيجية النمسا التي أكدت أنه يمكن أن يُرتكب الإرهاب السيبراني من جهات فاعلة حكومية أو غير حكومية، فما زال الأمر يحتاج إلى ضبط لتعريفهما، فقد ترتكب دولة هجوماً سيبرانياً ضد دولة أخرى لتحقيق نفس أغراض الإرهاب السيبراني التي قد تتمثل في الترويع أو الإجبار للحكومات أو للمجتمعات لتحقيق أغراض سياسية، إلا أن آثار ذلك الهجوم قد يحدث تدميراً للبنى التحتية وضرراً مشابهًا للحرب الفعلية، فهل يُطلق عليه إرهاب سيبراني أم حرب سيبرانية؟

أولاً: أشهر الهجمات السيبرانية 2020 تؤكد التداخل بين الإرهاب السيبراني والحروب السيبرانية:

في 13 ديسمبر 2020 تعرضت الولايات المتحدة الأمريكية لأسوأ هجوم سيبراني حكومي على الإطلاق، وهو ما يسمى بهجوم Solar Winds [2]، فقد تم استهداف الوكالات الفيدرالية الرئيسية،

(1) Congressional Research Service, "Defense Primer: Electronic Warfare", Updated October 29, 2020. https://fas.org/sgp/crs/natsec/IF11118.pdf - Updated November 23, 2021. https://sgp.fas.org/crs/natsec/IF11118.pdf

(2) Josh Fruhlinger, "What is a cyber-attack? Recent examples show disturbing trends"FEB 27, 2020. https://www.csoonline.com/article/3237324/what-is-a-cyber-attack-recent-examples-show-disturbing-trends.html

من وزارة الأمن الداخلي إلى الوكالة التي تشرف على ترسانة الأسلحة النووية الأمريكية وشركات التكنولوجيا والأمن القومي بما في ذلك Microsoft، وبدأ الاختراق عندما تم التسلل إلى تحديثات برمجية ضارة لبرنامج مشهور يسمى Orion، من إنتاج شركة Solar Winds، فقد تم الكشف عن أن شركة (Austin) أوستن وهي شركة برمجيات إدارة تكنولوجيا المعلومات، التي توفر مراقبة الشبكة والخدمات الفنية الأخرى لمئات الآلاف من المنظمات حول العالم ومقرها سولارويندز (Solar Winds)، قد تعرضت لهجوم من سلسلة التوريد أدى إلى اختراق التحديثات لمنصة برمجيات أوريون (Orion software platform) التابعة لها، أدخل المهاجمون البرامج الضارة الخاصة بهم المعروفة الآن باسم Sunburst أو Solorigate في التحديثات، والتي تم توزيعها على العديد من عملاء Solar Winds الضحية الأولى المؤكدة كانت شركة الأمن السيبراني FireEye، أظهرت التحقيقات أن المتسللين الذين يُعتقد أنهم تحت رعاية حكومة إحدى الدول [1]، ولم يتم التوصل إلى دليل قاطع على إدانة تلك الدولة [2]، لطبيعة تلك الجرائم.

جدل قانوني في الأوساط الأمريكية حول تحديد طبيعة الهجوم هل هو إرهاب سيبراني- تجسس -أم حرب [3]؟

فقد وصفه السيناتور الأمريكي Dick Durbin ديك دوربين بأنه "إعلان حرب فعليًا"، لكن وصفه خبراء الأمن السيبراني والقانونيون إنه اختراق فلن يعتبر عملاً حربياً بموجب القانون الدولي لتطلب ذلك مستوى معينًا من القوة أو التدمير، لذا يدخل التاريخ باعتباره عملاً من أعمال التجسس، ويرى Duncan Hollis دنكان هوليس، أستاذ القانون في جامعة تمبل والمتخصص في الأمن السيبراني أن "الحرب تعني العنف والموت والدمار"، ويرى Hollis هوليس وخبراء آخرون أن الهجوم نفذ على ما يبدو لسرقة معلومات أمريكية حساسة، ويجب أن يُنظر إليه على أنه تجسس، كما ويرى Benjamin Friedman بنجامين فريدمان، مدير السياسات في مركز أبحاث "أولويات الدفاع": إن مجرد سرقة المعلومات، بقدر ما لا نحبها، ليس عملاً من أعمال الحرب بل يُعد تجسساً.

(1) Josh Fruhlinger, op.cit.

(2) David E. Sanger, "Russian Hackers Broke Into Federal Agencies, U.S. Officials "Dec. 13, 2020,Updated Feb. 9, 2021. https://www.csoonline.com/article/3237324/what-is-a-cyber-attack-recent-examples-show-disturbing-trends.html

(3) Jan Wolfe and Brendan Pierson," Suspected Russian Hack of U.S. Government: Espionage or Act of War?" insurance journal, December 21, 2020. https://www.insurancejournal.com/news/national/2020594810/21/12/.htm

ثانياً: تعريف الباحث للإرهاب السيبراني والحروب السيبرانية:

الإرهاب السيبراني: هو هجوم سيبراني الغرض منه تهديد الحكومات أو العدوان عليها، أو الإخلال بالنظام العام أو تعريض سلامة أو مصالح أو أمن المجتمع وأفراده للخطر، سعياً لتحقيق أهداف سياسية أو عقائدية أو أيدولوجية.

الحروب السيبرانية: هي هجوم سيبراني تقوم به دولة أو أحد من يعملون لمصلحتها على مرافق ومؤسسات البنى التحتية المدرجة عبر الفضاء السيبراني لدولة أخرى، يترتب عليه وقوع أضرار بالأمن القومي بمفهومه الشامل للدولة المعتدى عليها.

المحور الرابع
مفهوم الهجوم السيبراني

الهجوم السيبراني هو"[1] أي محاولة للوصول غير المصرح به إلى جهاز كمبيوتر أو نظام حوسبة أو شبكة كمبيوتر بقصد إحداث ضرر، وتهدف تلك الهجمات السيبرانية إلى تعطيل أو تدمير أو التحكم في أنظمة الكمبيوتر أو تغيير أو حظر أو حذف أو التلاعب أو سرقة البيانات الموجودة داخل هذه الأنظمة، فيمكن شن هجوم إلكتروني من أي مكان بواسطة أي فرد أو مجموعة أو منظمة أو دولة باستخدام واحدة أو أكثر من استراتيجيات الهجوم المختلفة أو تقنياته، اعتمادًا إلى حد كبير على ما إذا كانوا يهاجمون كيانًا مستهدفًا أو غير مستهدف، ففي الهجوم غير المستهدف، يحاول منفذو الهجوم السيبراني اقتحام أكبر عدد ممكن من الأجهزة أو الأنظمة، فيبحثون بشكل عام عن الثغرات الأمنية التي ستمكنهم من الوصول دون اكتشافهم أو حظرهم، أما في الهجوم المستهدف، يلاحق المهاجمون منظمة معينة، وتختلف الأساليب المستخدمة وفقًا لأهداف الهجوم، فعلى سبيل المثال، تم الاشتباه في مجموعة (Anonymous) أنونيموس الناشطة في مجال القرصنة في هجوم رفض الخدمة الموزع (DDoS) لعام 2020 على موقع إدارة شرطة (Minneapolis) مينيابوليس بعد وفاة رجل أسود أثناء اعتقاله من قبل ضباط مينيابوليس، وغالبًا ما تحدث الهجمات السيبرانية على مراحل، وغالباً ما يكون الدافع وراء تلك الهجمات السيبرانية هي المكاسب المالية والمعلومات[2].

(1) Mary K. Pratt," cyber-attack. January 2021. https://searchsecurity.techtarget.com/definition/cyber-attack#:~:text=A20%cyber20%attack20%is20%any,data20%held20%within20%these20%systems

(2) Dave Wallen," Types of Cyber Attacks: A Closer Look at Common Threats", October 6, 2020. https://securityboulevard.com/202010//types-of-cyber-attacks-a-closer-look-at-common-threats/

ولقد أورد القانون الاتحادي الإماراتي رقم 34 لسنة 2021 بشأن مكافحة الشائعات والجرائم الإلكترونية تعريفاً للهجمات السيبرانية بموجب المادة الأولى منه بأنها "كل استهداف متعمد ومُخطط للأنظمة المعلوماتية، أو البنية التحتية، أو الشبكات الإلكترونية، أو وسائل تقنية المعلومات يُقلل من قدرات ووظائف أي منها، سواء كان ذلك لغرض شخصي أو لأغراض الاعتراض أو التسلل أو الاختراق أو التسريب، أو بغرض تعريض البيانات أو المعلومات للخطر، أو تعطيل العمليات وما في حكمها"[1].

أسباب تزايد وتيرة الهجمات السيبرانية خلال العامين السابقين: فقد تزايدت وتيرة الهجمات السيبرانية سواء على منشآت ومراكز البنى التحتية للدول أو على المواقع أو الشبكات التابعة للأفراد أو شركات القطاع الخاص خلال العامين السابقين، ولعل أهم هذه الأسباب هو ضعف ثقافة الأمن السيبراني لدى المستخدمين وما قد ينجم عنها من ثغرات يستغلها المجرم السيبراني، وثاني هذه الأسباب ضعف البنى التحتية للأمن السيبراني لدى كثير من الدول، الأمر الذي ترتب عليه وجود نقاط ضعف وأصول رقمية دون حماية متطورة تواجه التقنيات التي يستخدمها المهاجمون في الاختراق والتسلل، وثالث هذه الأسباب جائحة كورونا المسمى بـ كوفيد 19، فقد ساعد النطاق غير المسبوق للعمل عن بُعد في جميع أنحاء العالم الناجم عن جائحة COVID-19 المجرم السيبراني على تكثيف شن هجماته، مستغلاً الخوف وعدم اليقين المرتبطين بتلك الجائحة، فضلاً عن نقاط الضعف الجديدة الناتجة عن التحول إلى الوضع الافتراضي، وفيما يلي[2] وقائع وهجمات وإحصائيات توثق تلك الأسباب السابق ذكرها، تضمنت تقارير CSO Online أن أكثر من 80% من الخروقات الأمنية كانت نتيجة لهجمات التصيد 60% من الخروقات الأمنية حدثت بسبب نقاط ضعف غير مصححة، زادت الهجمات على أجهزة إنترنت الأشياء بمقدار ثلاثة أضعاف في أوائل عام 2019، ووفقًا للبحث الذي أجرته جامعة مريلاند يحدث هجوم إلكتروني كل 39 ثانية في المتوسط، وهو ما يُترجم إلى 2244 هجومًا مذهلاً يوميًا، وأنه يتم فقدان أو سرقة ما يقرب من 7 ملايين سجل بيانات كل يوم واختراق 56 سجل بيانات كل ثانية استنادًا إلى التقرير، واختراق ما يقرب من 2,55 مليار سجل بيانات سنويًا، كما توقعت شركة Cybersecurity Ventures [3] للأمن السيبراني أن تقع الشركات في عام 2021 ضحية لهجوم برمجيات الفدية كل 11 ثانية، كما تعرضت

(1) الجريدة الرسمية الإماراتية، السنة 51 العدد 712(ملحق) .26-9-2021

(2) Dave Wallen," op.cit.

(3) Linn F. Freedman," Ransomware Attacks Predicted to Occur Every 11 Seconds in 2021 with a Cost of $20 Billion", The National Law Review, Volume XI, Number 82. March 23, 2021. https://www.natlawreview.com/article/ransomware-attacks-predicted-to-occur-every-11-seconds-2021-cost-20-billion

مؤسسات الرعاية الصحية لمزيد من الهجمات السيبرانية في ظل COVID-19،[1] فقد أفاد مركز شكاوى جرائم الإنترنت (IC3) التابع لمكتب التحقيقات الفيدرالي الأمريكي (FBI) أنه تلقى 12000 شكوى تتعلق بالتهديدات الإلكترونية لفيروس كورونا حتى شهر مارس 2020، و في مارس 2020 حذر المركز الكندي للأمن السيبراني من قراصنة ضارين يستهدفون قطاع الرعاية الصحية لديهم للوصول غير المصرح به إلى الملكية الفكرية والبحث والتطوير المتعلقين بـ COVID-19، أيضاً واجهت التشيك سلسلة من حوادث الأمن السيبراني على مرافق اختبار COVID-19، مما أدى إلى إنهاء العمليات ونقل المرضى إلى مستشفيات أخرى.

ووفقًا لتقرير المخاطر العالمية 2021 الصادر عن المنتدى الاقتصادي العالمي، تستمر المخاطر السيبرانية في الترتيب بين المخاطر العالمية، فقد أدت جائحة COVID-19 إلى زيادة تلك المخاطر، والكشف عن نقاط الضعف وعدم الاستعداد السيبراني، وتفاقم التفاوتات التكنولوجية داخل المجتمعات وفيما بينها [2].

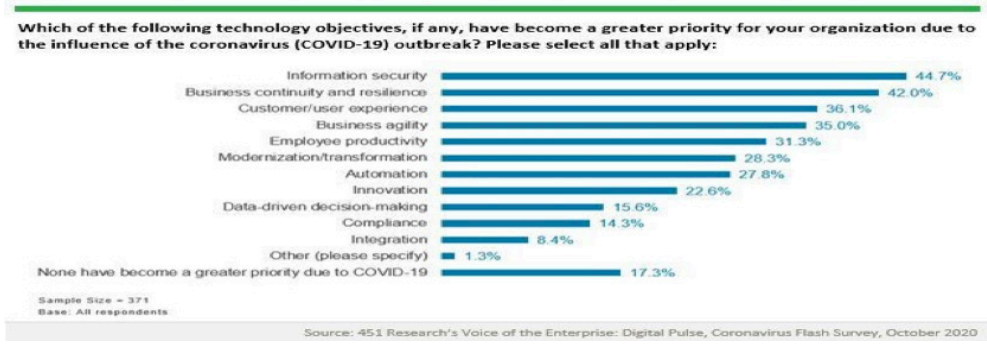


Image: Per S&P Global's 451 Research Voice of the Enterprise: Digital Pulse October 2020 Coronavirus Flash Survey, information security was the priority most often cited by respondents as having become greater due to COVID-19:

(1) Megan Hardiman," Corona Viruses and Computer Viruses: It's Time for a Cyber Health Check-Up", The National Law Review, Volume XI, Number 82. March 23, 2021. https://www.natlawreview.com/article/corona-viruses-and-computer-viruses-it-s-time-cyber-health-check

(2) Algirde Pipikaite, et, al "These are the top cybersecurity challenges of 2021", World Economic Forum, 21 Jan 2021. https://www.weforum.org/agenda/2021/01/top-cybersecurity-challenges-of-2021/

المحور الخامس
مظاهر الإرهاب السيبراني 2020-2021

تتعدد وتتنوع مظاهر الإرهاب السيبراني والتي تُجسد أساليب الهجمات السيبرانية وذلك حسب ما ذكرنا من قبل نوع الهدف المطلوب تحقيقه وحسب حجم وطبيعة الهدف المطلوب إصابته ومدى قوة الأمن السيبراني المتوافرة، فدائماً ما يبحث المهاجمون السيبرانيون أو المتسللون على نقاط ضعف أو نقاط دون حماية لشن هجماتهم، وسوف نتناول أشهر تلك الأساليب وأخطرها كالتالي[1]:

أولاً: هجمات الهندسة الاجتماع Social Engineering Attacks:

في مجال أمن المعلومات، تعتبر الهندسة الاجتماعية مصطلحًا شاملاً لمجموعة واسعة من الأنشطة الضارة على النحو التالي:

-التصيد الاحتيالي: Phishing هو أحد أكثر هجمات الهندسة الاجتماعية استغلالًا، حيث يرسل المهاجمون رسائل بريد إلكتروني ضارة تحتوي على روابط قابلة للنقر*التصيد بالرمح: Spear Phishing مثل التصيد الاحتيالي، يعد التصيد بالرمح نوعًا من هجمات البريد الإلكتروني الموجهة والمخصصة*التصيد الصوتي: (Vishing) يُعرف أيضًا voice phishing، وهو يتضمن قيام المحتالين بإجراء مكالمات هاتفية أو ترك رسائل صوتية لخداع الأفراد لإفشاء معلومات حساسة*الاصطياد: Baiting كما يوحي الاسم يطعم المهاجم الفرد ليقوم بعمل مرغوب فيه مقابل شيء ما*هجوم "شيء مقابل شيء ما" Quid Pro Quo: حيث يقدم المتسللون مساعدة أو خدمة مجانية مقابل الحصول على معلومات أو أموال مهمة.

ثانياً: هجمات البرمجيات الخبيثة Malware Attacks:

هجمات البرامج الضارة هي أكثر أنواع الهجمات شيوعًا حيث ينشئ المجرمون الإلكترونيون برامج ضارة بهدف إلحاق الضرر بالأجهزة أو البيانات أو الشبكة الحساسة للضحية دون علمه، ويتم تنفيذها على جميع أنواع الأجهزة وأنظمة التشغيل من أجل الوصول إلى المعلومات وسرقة البيانات، ويصعب اكتشاف هذه الأنواع من الهجمات مثل:

- برامج الفدية (Ransomware) يطور المجرم السيبراني برامج ضارة لمنع الوصول إلى ملفات أو بيانات الضحية ويطلبون فدية لتسليم الملفات المخترقة.

(1) Dave Wallen," op.cit.

- هجوم Drive-By، يستخدم هذا الهجوم تطبيقات أو أنظمة تشغيل أو متصفحات ويب غير آمنة، يقوم المهاجمون بتضمين برنامج نصي ضار على صفحات موقع الويب الذي يقوم تلقائيًا بتشغيل المتصفح لتنزيل البرامج الضارة عندما يزور الضحية موقع الويب المصاب.
- أحصنة طروادة: (Trojans) تبدو هذه الأنواع من برامج الكمبيوتر شرعية وتخدع المستخدمين لتنزيل التطبيقات الضارة، يمكن أن تؤدي هذه الهجمات إلى تعطل جهاز الضحية أو الكشف عن البيانات الشخصية.
- برامج الإعلانات المتسللة: (Adware)، وهي نوع من البرامج الضارة التي توجد سراً على نظام الهدف وتعرض إعلانات غير مرغوب فيها أو غير ذات صلة، ويمكن لها إتلاف جهاز الضحية أو مراقبة النشاط أو إصابة المتصفحات أو تثبيت الفيروسات.
- برامج التجسس: (Spyware) هي برامج ضارة تُستخدم لجمع المعلومات ومراقبة النشاط دون علم المستخدم.
- رفض الخدمة (DoS) ورفض الخدمة الموزع (DDoS) يتم تنفيذه عن طريق التحميل الزائد على الجهاز أو الشبكة المستهدفة بحركة مرور ضخمة، مما يجعل الخدمة غير متاحة للمستخدم، أيضاً يحدث عندما تغمر عدة أجهزة شبكة مصابة من مصادر مختلفة النطاق الترددي للنظام المستهدف، مما يتسبب في زعزعة استقراره أو تعطله، وهذا النوع من الصعب تحديد مصدر الهجوم، مثل هجمات SYN حيث يرسل المهاجم بشكل متكرر طلبات SYN لزيادة التحميل وإشباع موارد الخادم الهدف، مما يؤدي إلى بطء الاستجابة أو انعدامها.

ثالثاً: هجمات تطبيقات الويب:

Web Application Attacks وفيها يستغل المهاجمون نقاط الضعف في التطبيق للوصول إلى قواعد البيانات المتضمنة معلومات حساسة، مثل حقن SQLi: فيحاول الجناة الوصول إلى قاعدة البيانات عن طريق تحميل نصوص SQL غير موثوق بها، فتؤدي إلى تغيير أو حذف السجلات المخزنة في قاعدة بيانات SQL [1].

(1) (30) Josh Fruhlinger, op.cit

المطلب الثاني

الإرهاب السيبراني وتحديات الأمن القومي للدول

أولاً: مفهوم الأمن القومي وتطوره:

لم يعُد مفهوم الأمن القومي لمختلف دول العالم المتقدم قاصراً على تلك النواحي التقليدية العسكرية والأمنية، بل اتسع ذلك المفهوم وتطور لكي يتناسب مع حجم التحديات والتهديدات والمخاطر والأضرار التي ترتبت على إدراج مرافقه ومؤسساته في جميع النواحي والمجالات عبر ذلك الفضاء السيبراني، وما تتضمنه من أسرار ومعلومات وبيانات تتسم بالطابع الفني التقني يتم تداولها ومعالجتها والتعامل معها عبر تقنيات وآليات وفرضيات وتهديدات ذلك الفضاء السيبراني، وفي ذات الوقت تُمثل كيان الدولة ومؤسساتها ومرافقها، ومن ثم تُشكل مفردات للأمن القومي وجوانبه الرئيسية، الجانب العسكري، الاقتصادي، الصناعي، السياسي، البيئي، المائي، الغذائي، الصحي، الاجتماعي، الفكري، الأمن الشخصي أو الجسدي، الأمر الذي يعكس وبحق تهديداً حقيقياً وخطورة بالغة قد تعصف بكيان مؤسسات ومرافق الدول وفي ثوان معدودة ودون تحديد هوية المعتدي عبر ذلك الفضاء السيبراني.

ثانياً: ارتباط الأمن السيبراني بالأمن القومي:

وقد ترتب على إدراج مؤسسات ومرافق البنى التحتية عبر الفضاء السيبراني أن انتقلت أغلب الجرائم التقليدية بما فيها جرائم الإرهاب وجرائم أمن الدولة عبر ذلك الفضاء السيبراني، الذي أصبح يُمثل مسرح ارتكاب جريمتها، ويتطلب أدوات وأجهزة وتقنيات وكفاءات خاصة لجمع أدلتها وضبط مرتكبيها، من خلال قواعد معاينة تختلف اختلافاً جوهرياً عن قواعد معاينة مسرح الجرائم التقليدية، كما انتقلت فلسفة الصراع الدولي وتوازن أوراق اللعبة السياسية بين الدول عبر ذلك الفضاء، وتغيرت أشكال الحروب التقليدية بين الدول عبر تقنيات وشبكات وأجهزة اتصالات فرضها واقع ذلك الفضاء السيبراني، عابرة للحدود الدولية وآلية للتدمير عن بُعد، يوفر للدولة المعتدية الوقت والمال والجهد، ويُجنبها أي خسائر في الأموال أو المعدات العسكرية أو الأرواح، فبمجرد اكتشاف الثغرة الأمنية على الطرف الآخر من الكرة الأرضية يبدأ هجوم الدولة المعتدية وينتهي في ثوان معدودة، لتصبح تلك الحروب أكثر فتكاً وتدميراً لمؤسسات ومرافق الأمن

القومي للدول، وهو ما يُطلق عليه الحروب السيبرانية [1]، لذا فقد فرض واقع الحروب السيبرانية والإرهاب السيبراني وهجماتهم على البنى التحتية للدول ضرورة وجود منظومة قوية ومتطورة للأمن السيبراني لتأمين وحماية تلك البنى التحتية والتي تُشكل مفردات الأمن القومي لها، فتصدَر الأمن السيبراني على لائحة أولويات الأمن القومي للدول.

فقد وضعت دولة مثل الولايات المتحدة الأمريكية قضايا الأمن القومي على رأس أولوياتها، والتي لم تعد تقتصر على حماية حدود الدولة ضد التهديدات الخارجية والإرهاب، بل شملت قضايا جديدة مثل الجرائم السيبرانية والهجمات السيبرانية والجرائم الأخرى المستندة إلى الإنترنت، ويختص مكتب التحقيقات الفيدرالي (FBI) بصفته الوكالة الفيدرالية الرائدة في التحقيق في الجرائم السيبرانية، لأنها تهدد السلامة العامة والأمن الاقتصادي، كما تُعد خصوصية البيانات (Data Privacy) مصدر قلق كبير للأمن القومي لكل من الشركات والحكومة الفيدرالية، فيمكن أن يؤدي خرقه إلى إحداث فوضى في المخابرات والجيش والبيانات في مختلف مؤسسات البنى التحتية الأمريكية [2].

ثالثاً: تعريف الأمن السيبراني: [3]

عرَف الاتحاد الدولي للاتصالات (ITU) الأمن السيبراني بأنه "مجموعة الأدوات والسياسات والمفاهيم الأمنية وكذلك ضمانات الأمان والمبادئ التوجيهية وأساليب إدارة المخاطر والإجراءات والتدريب وأفضل الممارسات والضمان والتقنيات التي يمكن استخدامها لحماية البيئة السيبرانية وأصول المنظمة والمستخدم"، وأصول المؤسسة والمستخدم تتضمن أجهزة الحوسبة المتصلة والموظفين والبنية التحتية والتطبيقات والخدمات وأنظمة الاتصالات ومجموع المعلومات المرسلة أو المخزنة في البيئة الإلكترونية، كما جاء تعريفه بموجب المادة الأولى من القانون الاتحادي الإماراتي رقم 3 لسنة 2012 بشأن الهيئة الوطنية للأمن الإلكتروني بأنه "تأمين وحماية شبكة المعلومات، وشبكة الاتصالات ونظم المعلومات وعمليات جمع المعلومات باستخدام أي من الوسائل الإلكترونية"[4].

(1) د. عماد الدين محمد كامل عبد الحميد. استراتيجية تعزيز الأمن السيبراني للاقتصاد الرقمي- دراسة في العملات الرقمية للبنوك المركزية (CBDC). مجلة الاقتصاد الإسلامي، دبي، الجزء الثاني ص 25.

(2) Dr. Nick Oberheiden. "Defending Against National Security Threats," The National Law Review, Volume XI, Number 82. March 23, 2021. https://www.natlawreview.com/article/defending-against-national-security-threats

(3) د. عماد الدين محمد كامل عبد الحميد، المرجع السابق، ص 25.

(4) الجريدة الرسمية الإماراتية، 2012-8-13.

رابعاً: مؤشر الأمن السيبراني العالمي (Global Cybersecurity Index) (GCI) [1]:

هو مؤشر مركب وموجه موثوق به يصدر عن الاتحاد الدولي للاتصالات (International Telecommunication Union) (ITU) الذي يُعد إحدى وكالات الأمم المتحدة المتخصصة، من أجل قياس مدى التزام الدول بالأمن السيبراني على المستوى العالمي، لزيادة الوعي بأهمية الأمن السيبراني وأبعاده المختلفة في جميع المجالات، وقد اعتمد المؤشر خمس ركائز أساسية هي (تدابير قانونية – فنية – تنظيمية – بناء القدرات – التعاون)، من خلالها يتم تقييم مستوى الدول في قدراتها والتزامها بتحقيق الأمن السيبراني[2].

خامساً: ضعف منظومة الأمن السيبراني يهدد الأمن القومي للدول:

الهجمات السيبرانية التي تتعرض لها البنى التحتية المدرجة عبر الفضاء السيبراني لمختلف الدول، سواء اتخذت تلك الهجمات أشكال الحروب السيبرانية أو الإرهاب السيبراني، يتوقف نجاحها في تحقيق أهدافها على منظومة الأمن السيبراني ومدى قوتها وتطورها لمواجهه تلك الهجمات، فضلاً عن أن وجود منظومة ضعيفة للأمن السيبراني أو خلل في أحد مفرداتها قد يعرض الأمن القومي للخطر من قبل أشخاص قد يدفعهم حب الفضول للعبث بأحد مرافق الأمن القومي، فقد دفع حب الفضول المراهق البولندي آدم دابروفسكي (Adam Dabrowski) البالغ من العمر 14 عامًا في أوائل عام 2008 إلى اقتحام محطة الترام في مدينة لودز Lodz ليلاً، باستخدام جهاز تحكم عن بُعد قديم للتلفزيون بعد تحويله، مستغلاً خللاً في نظام الإشارات القائم على الأشعة تحت الحمراء والتقاط إشارة تبديل المسار عند نقطة تقاطع واحدة وتشغيلها مرة أخرى عند نقطة تقاطع أخرى

(1) ITU/BDT Cyber Security Programme, Global Cybersecurity Index (GCI), Guidelines for Member States, Version 0.9.04 September 2019. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv4/GCI_V4_Guidelines_for_Member20%States.pdf. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx#:~:text=As20%cybersecurity20%has20%a20%broad,(v)20%Cooperation%20%E220%93%80%and20%then

- يدعو قرار مؤتمر المندوبين المفوضين للاتحاد الدولي للاتصالات 1300 (المُراجع في دبي 20188) الدول الأعضاء إلى "دعم مبادرات الاتحاد بشأن الأمن السيبراني، بما في ذلك مؤشر الأمن السيبراني العالمي (GCI)، من أجل تعزيز الاستراتيجيات الحكومية وتبادل البيانات والمعلومات وتعزيز ثقافة عالمية للأمن السيبراني ودمجها في صميم تقنيات المعلومات والاتصالات، ويهدف GCI إلى تقليل الفجوة المرئية في مستوى مشاركة الأمن السيبراني بين مختلف المناطق حول العالم، فضلاً عن استخدامه كمرجع من قبل الدول الأعضاء في الاتحاد والبلدان الأخرى لتحسين التزامها بالأمن السيبراني.

(2) د. عماد الدين محمد كامل عبد الحميد. استراتيجية تعزيز الأمن السيبراني للاقتصاد الرقمي- دراسة في العملات الرقمية للبنوك المركزية (CBDC). مجلة الاقتصاد الإسلامي، دبي، الجزء الثاني العدد 486، إبريل 2021 ص 25. https://www.aliqtisadalislami.net/Els486.pdf/04/wp-content/uploads/2021

للحصول على نفس النتيجة[1]، وقد صرح المتحدث باسم شرطة لودز أن ذلك الهجوم قد أحدث فوضى وخروج بعض عربات القطار عن مسارها وحدوث إصابات لدى بعض الركاب[2].

سادساً: الإرهاب السيبراني وتهديدات الأمن القومي:

تشكل العمليات الإرهابية السيبرانية تهديداً خطيراً للأمن القومي لأن مؤسسات ومرافق البنى التحتية لمختلف دول العالم مدرجة عبر الفضاء السيبراني كما بينا، ولكونها هدفاً سهلاً وآمناً وغير مكلفٍ وناجحاً في تحقيق أهداف المعتدي وفي ثوان معدودة كما بينا من قبل، فالأنظمة المصرفية والمالية يتم تحويلها رقميًا ومتصلة بالإنترنت بشكل متزايد، ومن ثم تعرضها إلى الهجمات الإرهابية كما قرر خبراء الأمن السيبراني قد يؤدي إلى عدم استقرار اقتصادي واسع النطاق، مما قد يتسبب في ركود أو كساد، كما أنه من خلال اختراق البنية التحتية للطاقة أو المرافق، يمكن أن يتسبب الإرهابيون في حدوث فوضى في جميع أنحاء المناطق الحضرية الكبرى، وقد تمنع تلك الهجمات الوصول إلى شبكات الكمبيوتر التابعة لوزارة الدفاع بما في ذلك البريد الإلكتروني والأنظمة الحساسة الأخرى، وقد تمتد إلى صناعات الطاقة وتوليد الكهرباء وتوزيعها، بما في ذلك مصافي النفط وأنابيب النفط والغاز، أو التدخل في البنية التحتية الحيوية مثل خدمات الطوارئ، والمستشفيات، وتوليد الطاقة وتوزيعها، أو النقل، إلا أنه يُرجح أن منفذ تلك الهجمات بالفعل دول قوية، وأن دول مثل الصين وروسيا والولايات المتحدة هي مراكز قوة في الاستخدام الدفاعي والهجومي لتكنولوجيا المعلومات والاتصالات (ICT)، على الرغم من أن الدول الأخرى أكثر من قادرة على ذلك [3].

(1) John Bull, 'You Hacked: Cyber-Security and the Railways', London Reconnections, May 12, 2017. https://www.londonreconnections.com/2017/hacked-cyber-security-railways/

(2) John Leyden, 'Polish teen derails tram after hacking tram network', The Register, 11 Jan 2008. https://www.theregister.com/2008/01/11/tram_hack/

(3) Anjali C. Das,"U.S. Government Warns Companies of Legal Risk for Paying Ransom to Cybercriminals", The National Law Review, Volume XI, Number 83. March 24, 2021. https://www.natlawreview.com/article/us-government-warns-companies-legal-risk-paying-ransom-to-cybercriminals

سابعا: هجمات الإرهاب السيبراني على مرافق الأمن القومي للدول 2020-2021:

سوف نتناول بعض من تلك الهجمات بالقدر الي يتناسب مع جوهر البحث وشروطه وذلك على النحو التالي [1]:

- مارس 2021 شهد رئيس القيادة الإلكترونية الأمريكية أنها قد تعرضت لهجمات وتهديدات أجنبية قبل الانتخابات الأمريكية لعام 2020.
- قيام متسللين صينيين بحملة تجسس إلكتروني ضد قطاع النقل الهندي.
- أعلنت أجهزة الأمن البولندية أن قراصنة روس مشتبه بهم استولوا لفترة وجيزة على المواقع الإلكترونية للوكالة الوطنية للطاقة الذرية ووزارة الصحة في بولندا، لنشر تنبيهات كاذبة عن وجود تهديد إشعاعي غير موجود.
- استهدف جهازا المخابرات الروسية والصينية وكالة الأدوية الأوروبية لسرقة وثائق تتعلق بلقاحات وأدوية COVID-19.
- في فبراير2021 استهدف قراصنة كوريون شماليون شركات دفاعية في أكثر من اثنتي عشرة دولة في حملة تجسس بدأت في أوائل عام 2020.
- اخترق المتسللون الروس نظام مشاركة الملفات التابع للحكومة الأوكرانية.
- حاول قراصنة مجهولون رفع مستويات هيدروكسيد الصوديوم في إمـدادات المياه في أولدسمار بولاية فلوريدا بمعامل 100 عن طريق استغلال نظام الوصول عن بعد، وفي يناير 2021 اخترق قراصنة مجهولون أحد مراكز البيانات التابعة للبنك المركزي النيوزيلندي، وفي ديسمبر 2020 استهدف قراصنة صينيون البرلمان الفنلندي، وخرقوا حسابات البريد الإلكتروني لأعضاء البرلمان وغيرهم من الموظفين.
- وفي نوفمبر2020 استهدف القراصنة الصينيون المنظمات اليابانية في قطاعات صناعية متعددة تقع في مناطق متعددة حول العالم، وفي أكتوبر 2020 كشفت وزارة الأمن الداخلي الأمريكية أن المتسللين استهدفوا مكتب الإحصاء الأمريكي في محاولة محتملة لجمع بيانات مجمعة أو تغيير معلومات التسجيل أو اختراق البنية التحتية للتعداد أو شن هجمات DoS[2].

(1) Center for Strategic &International Studies, (CSIS), Significant Cyber Incidents. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents. https://csis-website-prod.s3.amazonaws.com/s3fs-public/210326_Significant_Cyber_Events.pdf?ZKJIdGVXdQd2vXW.gFEcFQs2Ay7cDiqt

(2) د. عماد الدين محمد كامل عبد الحميد، المرجع السابق، الجزء الثاني العدد 486، إبريل 2021 ص 26.

المبحث الثاني

الإرهاب السيبراني المرتبط بالطائرات المسيرة

تمهيد:

نتناول دراسة هذا المبحث من خلال مطلبين، المطلب الأول لدراسة ماهية الطائرات المسيرة (Drones) نتناول تعريفها ومكونات البنى التحتية لها، ثم أنواعها وتعدد وتنوع استخداماتها، والتنظيم القانوني للطائرات المسيرة في دولة الإمارات، ثم نتناول في المطلب الثاني الهجوم السيبراني باستخدام الطائرات المسيرة وتهديدات الأمن القومي، ببيان تهديد الطائرات المسيرة لمرافق الأمن القومي، واستخدامها في عمليات التجسس والقرصنة والعمليات الإرهابية والتهريب والعمليات الإرهابية، ثم بيان الهجوم السيبراني الواقع على الطائرات المسيرة، وذلك كله على النحو التالي:

المطلب الأول

ماهية الطائرات المسيرة (Drones)

أولاً: تعريف الطائرات المسيرة:

عرفت المنظمة الدولية للطيران المدني الأيكاو (ICAO)[1] الطائرات المسيرة بأنها "طائرة تُصنع لغرض الطيران بدون قائد على متنها، ويمكن تشغيلها والتحكم الكامل بها عن بُعد ومكان آخر في الأرض أو من طائرة أخرى أو من الفضاء، وقد تكون مبرمجة ذاتيا بحيث يمكن أن تقوم بالرحلة الجوية دون أي تدخل خارجي"، كما أوردت منظمة الأيكاو أنه على الرغم من أن مصطلح (DRONE) يستخدم بشكل شائع للإشارة إلى هذه الطائرات، إلا أن بعض الدول عند وضع اللوائح والقواعد الإرشادية لتنظيم تلك الطائرات قد تستخدم مصطلح UA (unmanned aircraft)، أو مصطلح RPA (remotely piloted aircraft) للإشارة إليها، فقد استخدمت إدارة الطيران الفيدرالية الأمريكية (FAA)[2] مصطلح UA (unmanned aircraft) وعرفتها بأنها "جهاز يستخدم أو يعتزم استخدامه للطيران في الهواء بدون طيار على متنه، يستثني هذا الجهاز الصواريخ أو

(1) ICAO, "UNITING AVIATION "A United Nations Specialized Agency. https://www.icao.int/about-icao/Pages/default.aspx.

(2) The Federal Aviation Administration (FAA). Nov 6, 2020. https://www.faa.gov/uas/espanol/glosario/

الأسلحة أو الرؤوس الحربية المتفجرة، ولكنه يشمل المناطيد وطائرات الرفع الآلية بدون طيار على متنها، ولا تشمل UA البالونات التقليدية والصواريخ والطائرات المربوطة والطائرات الشراعية غير المزودة بالطاقة، كما استخدمت مصطلح (Unmanned aircraft system UAS) وأطلقته على الطائرة بدون طيار والعناصر المرتبطة بها، والتي تشمل محطات التحكم (الأرضية أو السفن أو الجوية)، ووصلات التحكم، ومعدات الدعم، والحمولات، وأنظمة إنهاء الرحلة، ومعدات الإطلاق والاسترداد، ويتكون UAS من ثلاثة عناصر: طائرات من دون طيار، محطة التحكم، وصلة البيانات. وفي دولة الإمارات العربية المتحدة فقد عرفت الهيئة العامة للطيران المدني الطائرات المسيرة بأنها "هي أنظمة الطائرات بدون طيار وجميع العناصر المرتبطة بها، كجهاز الاتصال والاستقبال وأجهزة التصوير، والتي يُنوى الطيران بها بدون وجود طيار على متنها، ولا يشمل ذلك البالون أو الطائرات الورقية"[1]، ولقد أصدرت حكومة دبي قانون تنظيم الطائرات بدون طيار في إمارة دبي، وهو القانون رقم 4 لسنة 2020 ولقد ورد في المادة الثانية منه تعريفاً للطائرة بدون طيار بأنها "طائرة تُحلق في الجو دون وجود القائد على متنها، وتشمل الطائرة الموجّهة بالعين المجرّدة، والطائرة الموجّهة عن بُعد، والطائرة المسيّرة ذاتيّاً، والطائرة الموجّهة بالعين المجرّدة هي طائرة بدون طيّار يتم التحكُم بها بواسطة جهاز لاسلكي، والسيطرة عليها بالعين المُجرّدة من قائد الطائرة بدون طيار، أما الطائرة الموجّهة عن بُعد هي طائرة بدون طيّار يتم التحكُم بها لاسلكيّاً، والسيطرة على حركتها من خلال محطّة التحكم عن بُعد، والطائرة المسيّرة ذاتيّاً هي طائرة بدون طيّار يتم التحكُم بها عن طريق برمجتها، والسيطرة على حركتها ذاتيّاً"[2].

ثانياً: بنى الطائرات بدون طيار:

تقوم بنية الطائرات بدون طيار على ثلاثة عناصر، وحدة التحكم في الطيران، محطة التحكم الأرضية، روابط البيانات [3]: **الأول وحدة التحكم في الطيران (Flight Controller):** تم تصنيفها على أنها وحدة المعالجة المركزية للطائرة بدون طيار.

الثاني محطة التحكم الأرضية: (Ground Control Station) (GCS) وهي تعتمد على منشأة على الأرض (On-Land Facility) (OLF) والتي تزود المشغلين البشريين بالقدرات اللازمة

(1) الهيئة العامة للطيران المدني دولة الإمارات https://www.gcaa.gov.ae/ar/pages/uas.aspx

(2) الجريدة الرسمية لحكومة دبي، عدد خاص بـ شؤون الطيران المدني، السنة 54، العدد 479، 7 يوليو 2020.

(3) Jean-Paul Yaacoub, et, al," Security analysis of drones' systems: Attacks, limitations, and recommendations", US National Library of Medicine National Institutes of Health,2020 Sep. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7206421/

للتحكم ومراقبة الطائرات بدون طيار أثناء عملياتهم من مسافة بعيدة، تختلف أنظمة GCS اعتمادًا على الحجم والنوع ومهام الطائرات بدون طيار، الثالث روابط البيانات: (Data Links) هي روابط لاسلكية تستخدم للتحكم في تدفق المعلومات بين الطائرة بدون طيار ونظام GCS هذا يعتمد على المدى التشغيلي للطائرات بدون طيار، ويمكن تصنيف تحكم الطائرات بدون طيار بناءً على بعدها عن محطة التحكم الأرضية (GCS) إلى:

- مسافة خط البصر المرئي: (Visual Line-of-sight (VLOS) Distance) تتيح إرسال إشارات التحكم واستقبالها عبر استخدام موجات الراديو المباشرة.
- ما وراء خط البصر Beyond Visual Line-of-Sight (BVLOS) Distance: يسمح بالتحكم في الطائرات بدون طيار عبر اتصالات الأقمار الصناعية.

ثالثاً: أنواع الطائرات المسيرة وتعدد وتنوع استخداماتها:

لا يوجد معيار واحد يتم على أساسه تصنيف أنواع الطائرات بدون طيار فهناك عدة معايير، وفقاً لمعيار الاستخدام تتعدد أنواعها إلى الطائرات بدون طيار لغرض التسلية أو الترفيه، وتلك التي تستخدم في الأغراض التجارية والصناعية، والطائرات التي تستخدم من قبل الدول في أغراض مدنية، ووفقاً لمعيار التحكم في الطائرة فهناك الطائرات بدون طيار التي يتم التحكم بها يدوياً، وتلك التي تتحرك إلكترونياً بموجب برنامج مُعد مسبقاً هو الذي يتحكم بها دون تدخل الطيار، وأخرى تتحرك إلكترونياً بموجب تحكم برنامج مع السماح بالتدخل للطيار، ومن حيث معيار الخصائص المكلَفة بها تتعدد وتتنوع الطائرات بدون طيار من حيث الوزن والمدى، وارتفاعها، ونوع المحرك وقدرة الدفع وغيرها[1].

ويتنوع استخدام الطائرات المسيرة في جميع المجالات، مجال التصوير الجوي للصحافة والسينما، الشحن السريع والتسليم، جمع المعلومات أو توفير الأساسيات لإدارة الكوارث، طائرات بدون طيار ذات استشعار حراري لعمليات البحث والإنقاذ، رسم الخرائط الجغرافية للتضاريس والمواقع التي يتعذر الوصول إليها، تفتيش سلامة المباني، نقل البضائع بدون طيار، مراقبة إنفاذ القانون ومراقبة الحدود، تتبع العواصف والتنبؤ بالأعاصير، إسعاف الحالات الطارئة خاصة في الحالات التي يكون فيها التدخل البشري غير آمن، كما في حالة انقلاب قارب أو غرق شخص، فيمكن للمركبة ذاتية القيادة تحت الماء (AUV) المساعدة في الإنقاذ، وأيضاً إذا كان هناك انهيار جليدي، يتم

(1) Vinay Chamola, a, b Pavan Kotesh, et al" A Comprehensive Review of Unmanned Aerial Vehicle Attacks and Neutralization Techniques", US National Library of Medicine, National Institutes of Health, Search database, , 2021 Feb 1. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7547616/

نشر طائرات بدون طيار للبحث عن الأشخاص وسط ذلك الانهيار، كما تُستخدم في الجو لتتبع مجموعات الحياة البرية ومجموعات الحيوانات المتجولة مع صعوبة نجاح المهمة في حال وجود الإنسان على الأرض، و تُستخدم لرسم خرائط ثلاثية الأبعاد للمواقع التاريخية[1]، وفي مجال الإدارة البيئية لأداء مهام قياس التلوث في عناصر البيئة، وفي المهام الزراعية لتحليل التربة - والمحاصيل - إدارة البذور - الثروة الحيوانية ومكافحة الآفات، كما تستخدم لمراقبة حركة المرور ومشاهد الحوادث ومراقبة الهاربين من مسرح الجريمة والسجون، كما تم استخدامها في دولة الإمارات من قبل مأموري الضبط القضائي لأغراض البحث والتحري وضبط الجرائم وملاحقة مرتكبيها.

رابعاً: التنظيم القانوني للطائرات بدون طيار في دولة الإمارات:

تختص الهيئة العامة للطيران المدني في دولة الإمارات (GCAA) بالتنظيم والإشراف والرقابة والمساءلة بشأن الطائرات بدون طيار على اختلاف أنواعها واستخداماتها، في مواجهة جميع الأفراد والجهات العامة والخاصة، وذلك بالتنسيق مع الجهات الحكومية المعنية الأخرى في الدولة، وذلك عبر منظومة تشريعات وأنظمة لعمل الطائرات بدون طيار، وممارستها سواء لأغراض تجارية أو ترفيهية، والهدف من هذه الأنظمة تأمين السلامة الجوية والبرية، بالإضافة إلى حماية خصوصية الأفراد وأمن بياناتهم، وتتضمن تدابير الأمن والسلامة التي يفرضها قانون الهيئة، ضرورة التسجيل والحصول على ترخيص، وحظر الطيران في أماكن معينة، وشروط خاصة بالمشغل المخول بالإشراف على الطائرة بدون طيار، والعقوبات التي تنجم عن الإخلال بالتقيد بأحكام القوانين والأنظمة التي تفرضها الهيئة، كما صادقت الهيئة الاتحادية للطيران المدني وهيئة دبي للطيران المدني على تشريعات وأنظمة تحظر استخدام الطائرات بدون طيار قرب، أو حول، أو فوق المطارات، ولغرض حماية خصوصية السكان تحظر السلطات الاتحادية والبلدية تحليق الطائرات بدون طيار فوق المناطق السكنية، وأصدرت هيئة الطيران المدني الاتحادية تطبيقاً يتضمن خريطة إلكترونية لتحديد المناطق التي يُسمح أو يُحظر فيها استخدام أو تشغيل الطائرات بدون طيار أو الطائرات المُوجهة، ويمكن للتطبيق بمجرد تشغيله، التأكيد فيما إذا كانت المنطقة التي يوجد فيها المستخدم، تخضع لحظر ممارسة أنشطة الطائرات من دون طيار أم لا، كما يتعين على مستخدمي تلك الطائرات الحصول أولاً على شهادة عدم ممانعة من الجهة المختصة، وعليهم معرفة الأنظمة والقيود المرعية بشأن استخدام الطائرات بدون طيار، والتي تخص كل إمارة بنفسها، كما يجب تسجيل جميع الطائرات بدون طيار لدى الهيئة الاتحادية للطيران المدني (GCAA)، عبر الإنترنت،

(1) Drones, What Is A Drone? What Are Uses For Drones? April 2021. https://builtin.com/drones

كما أطلقت هيئة المواصفات والمقاييس منصة إلكترونية موحدة لتسجيل الطائرات بدون طيار والمركبات الجوية التي تستخدم في أجواء الدولة للأغراض الترفيهية والخدمية والتجارية، ووفقاً للوائح الهيئة يتعين على التجار والموردين والموزعين للطائرات بدون طيار تسجيل منتجاتهم عبر الإنترنت من خلال المنصة الموحدة لتسجيل الطائرات بدون طيار، وستعنى المنصة بالحصول على معلومات الطائرات بدون طيار، ومطابقتها مع المواصفات القياسية الإماراتية، وتتيح هذه الخدمة أيضاً تسجيل الطائرات بدون طيار في نفس الوقت مع ثلاث جهات حكومية أخرى تشرف على ملكية وأنظمة وتشغيل هذه الطائرات واستخدامها وسلامتها في الدولة، وهذه الجهات هي وزارة الداخلية، والهيئة العامة لتنظيم قطاع الاتصالات، والهيئة العامة للطيران المدني، وستصدر هيئة الإمارات للمواصفات والمقاييس شهادة رقمية لكل طائرة بدون طيار مسجلة لإثبات أنها تلبي المعايير الوطنية ويمكن بيعها بشكل قانوني في الدولة، وسيكون لكل طائرة بدون طيار مسجلة رقم تسلسلي مميز يربطها بمصنعها وموزعها والعميل النهائي الذي يشتريها، بحيث يمكن تتبع الدورة الكاملة للطائرة بدءاً من الشركة المصنعة ولغاية المستخدم النهائي، فعند بيع الطائرة أو التنازل عنها يكون من خلال المنصة الموحدة لتسجيل الطائرات بدون طيار "My Drone" لنقل الملكية إلى المشتري الجديد، كما يوجد لدى الهيئة الاتحادية للطيران المدني (GCAA) تطبيق شامل لمستخدمي أنظمة الطائرات بدون طيار (UAS)، وأنظمة الطائرات التي يتم قيادتها عن ُبعد (RPAS) وطائرات بدون طيار (Drones) لإعلامهم ومساعدتهم في استخدام طائراتهم بالامتثال مع لوائح سلامة الطيران، كما يتيح هذا التطبيق تسجيل الطائرات بدون طيار في الدولة، ويتيح التطبيق الذكي والذي يطلق عليه (My Drone Hub) في عملية التحديد الفوري للمناطق التي يسمح التصوير بها، مع التركيز على سلامة وأمن حركة الطيران والمنشآت الوطنية، ومراعاة خصوصية الأفراد والممتلكات، ويخصص فقط لحاملي الهوية الصادرة من الهيئة الاتحادية للهوية والجنسية، ويساعد التطبيق في تحديد موقع جميع المعلومات للمستخدمين من خلال خريطة تفاعلية، ويمكن للمستخدم النقر فوق أي مكان في الخريطة للتحقق من الامتيازات الموجودة في المنطقة المحددة، هذا التطبيق مُتاح على منصة (iTunes) [1].

قانون حكومة دبي 4 لسنة 2020 بشأن تنظيم الطائرات بدون طيار: حددت المادة الثالثة نطاق تطبيق أحكام هذا القانون، ليُطبق على كل أنحاء الإمارة وعلى جميع أنواع الطائرات بدون طيار واستخداماتها باختلاف أنظمة التحكم فيها، ويخضع له جميع الأفراد والجهات العامة والخاصة التي تستخدم الطائرات بدون طيار في الإمارة، ويُستثنى من تطبيق أحكام هذا القانون الطائرات

(1) موقع حكومة دولة الإمارات العربية المتحدة – سلامة الطيران، تحديث 19 فبراير 2020. https://u.ae/ar-AE/information-and-services/justice-safety-and-the-law/aviation-safety .

بدون طيار التي يتم استخدامها للأغراض العسكرية على أن يتم التنسيق مع هيئة دبي للطيران المدني لضمان سلامة عمليات التشغيل، وعدم تعريض سلامة الطيران المدني للخطر، كما أسند القانون بموجب المادة الخامسة الاختصاص لهيئة دبي للطيران المدني المدنية الإشراف على تطبيق أحكامه، وتنظيم عمليات التشغيل والأنشطة المرتبطة، بما يتفق مع التشريعات الاتحادية والمعاهدات والاتفاقيات التي تكون الدولة طرفاً فيها، فلها كل الاختصاصات المتعلقة بعمليات التشغيل والأنشطة المرتبطة والإشراف والرقابة عليها، ووضع واعتماد الشروط والإجراءات اللازمة لإصدار التصاريح، تحديد واعتماد المناطق المعتمدة والارتفاعات المسموح بها، اعتماد المجالات والمسارات الجوية، اعتماد شروط ومعايير إنشاء المطارات الخاصة ونظم وخدمات أمن وسلامة وبيئة الطيران لتلك الطائرات، كما تتولى مؤسسة دبي لخدمات الملاحة الجوية بموجب المادة السادسة تحديد المجال الجوي الخاص بالطائرات بدون طيار، وتقديم خدمات الملاحة الجوية لها لتحقيق أمن وسلامة حركة الملاحة الجوية وحركة الطائرات بدون طيار، فضلاً عن التصميم المتعلق بالمجالات والمسارات الجوية التي يُسمح للطائرات بدون طيار التحليق فيها بالتنسيق مع الهيئة وبما لا يؤثر على أمن وسلامة المجال الجوي، ويتولى جهاز الشرطة بموجب المادة الثامنة وبالتنسيق مع الهيئة سن وتطبيق الإجراءات والتدابير الأمنية للتصدي والوقاية من أفعال التدخل غير المشروع المتعلقة باستخدام الطائرات بدون طيار وكذلك التحقيق في الجرائم الناتجة عن استخدامها، وضع وتطبيق الإجراءات والتدابير الوقائية في حال فقدان السيطرة على الطائرة بدون طيار أو خروجها عن المناطق المعتمدة أو المسارات الجوية أو عدم امتثالها لتعليمات الهيئة والجهات المعنية، كما نصت المادة العاشرة على حظر استخدام الطائرة بدون طيار، أو قيادتها، أو القيام بعمليات التشغيل، أو مزاولة أي من الأنشطة المرتبطة، أو إنشاء البنية التحتية، أو إنشاء مطار خاص بالطائرات بدون طيار في الإمارة دون الحصول على الترخيص، كما أسندت المادة الثانية عشرة الاختصاص لمدير هيئة دبي للطيران المدني بتحديد أنواع وفئات الطائرات بدون طيار التي يجوز تشغيلها في الإمارة والشروط والمتطلبات والمواصفات الواجب توفُرها فيها، وأسندت المادة التاسعة عشرة الاختصاص للهيئة بالتنسيق بينها وبين الهيئة الاتحادية لتنظيم قطاع الاتصالات بوضع شروط ومتطلبات وإجراءات استخدام الترددات الراديويّة الخاصة بالطائرات بدون طيار وأنظمتها ومحطات التحكم عن بُعد، فقد نص القانون على مجموعة من الإجراءات والتدابير والاشتراطات الواجبة والالتزامات الواقعة على أطراف منظومة الطائرات بدون طيار سواء تعلق الأمر بالحيازة أو الاستخدام أو التشغيل أو استخدام المجال الجوي، أو التدخل غير المشروع والخصوصية وحماية البيانات والبيئة، وقررت المادة 38 عقوبة الحبس والغرامة أو إحدى هاتين العقوبتين جزاء لمخالفة أحكامه.

المطلب الثاني

الهجوم السيبراني باستخدام الطائرات المسيرة وتهديدات الأمن القومي

أولاً: تهديد الطائرات المسيرة لمرافق الأمن القومي:

أصبحت الطائرات المسيرة مصدر تهديد خطير لمرافق الأمن القومي نظراً للتقنيات والإمكانيات الرهيبة لتك الطائرات التي يُطالعنا سوق منتجاتها وصناعتها كل يوم بالجديد والغريب، فيمكن للطائرات بدون طيار أن تطير فوق الأسوار والجدران ويمكن أن تفلت بتقنياتها وصغر حجمها من أنظمة الرادار التقليدية، لإمكانية نقلها في صندوق السيارة أو في حقيبة الظهر، كما يمكن إطلاقها من أي حديقة أو موقف للسيارات أو شارع بالمدينة أو طريق سريع عام، وبمجرد أن تُحلق طائرة بدون طيار في الجو، يمكن أن تصل في غضون دقائق إلى أي مكان على بعد بضعة كيلومترات من موقع الإطلاق، ومن ثم يضعف ضبط وملاحقة الجناة، كما أمكن التحكم في صناعة تلك الطائرات وتزويدها بالأجهزة والتقنيات المتطورة لكي تقوم بالمهام الموكلة إليها، سواء تزويدها بتقنيات مراقبة متطورة أو بأجهزة تنصت أو بكاميرات دقيقة تستطيع أن تُسجل كل ما يدور بالصوت والصورة في المكان المراقب، ومن مسافات بعيدة، أو تزويدها بأجهزة استشعار عن بُعد، أو أجهزة لها القدرة على رسم الخرائط الجغرافية ثلاثية الأبعاد للتضاريس والمواقع المهمة والحساسة، وإرسال النتائج والتقارير إلى مراكز التحكم أو القيادة في ثوان معدودة، كما يمكن لتلك الطائرات القيام بالهجوم السيبراني لخرق منظومة الأمن السيبراني لأي مرفق أو مؤسسة للبنى التحتية لمختلف دول العالم مدرجة عبر الفضاء السيبراني أو تقع خارج منظومة ذلك الفضاء، سواء لاستراق البيانات والمعلومات أو تدميرها أو الاستيلاء على مراكز التحكم والسيطرة وتوجيه ذلك المرفق إلى تحقيق الهدف المطلوب أو جعله خارج نطاق الخدمة.

ثانياً: استخدام الطائرات المسيرة في التجسس والقرصنة والتهريب والعمليات الإرهابية [1]:

فيما يتعلق بعمليات التجسس تحتوي العديد من الطائرات بدون طيار على كاميرا عالية الدقة

(1) Vinay Chamola, a, b Pavan Kotesh, et al" A Comprehensive Review of Unmanned Aerial Vehicle Attacks and Neutralization Techniques", US National Library of Medicine, National Institutes of Health, Search database, , 2021 Feb 1. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7547616/

ملحقة بها لنقل لقطات حية إلى المستخدم، ففي ديسمبر 2016 في Orem, Utah, الولايات المتحدة الأمريكية تم العثور على طائرة بدون طيار مع مقطع فيديو تم التقاطه لعدة أشخاص في منازلهم[1]، تتجسد خطورة ذلك فيما لو كان في محل الواقعة اجتماع أمني في مؤسسة أمنية، كما تم استخدام الطائرات بدون طيار لتتبع مسؤولي إنفاذ القانون لتوقع تحركاتهم، والتخطيط للجرائم خاصة السرقات، و استخدامها على الحدود الوطنية لتتبع دوريات الحدود لتجنبها أثناء العبور [2].

وفيما يتعلق بعمليات التهريب يمكن للطائرات بدون طيار الصغيرة التي يستخدمها الهواة أن يكون لديها 0.3 إلى 2 كجم من سعة الحمولة، ومن ثم يمكن استخدامها لحمل المتفجرات والمخاطر البيولوجية، وعلى الرغم تجريم الدول لذلك إلا أنه في أحوال كثيرة يتعذر تحديد المالك أو مشغل الطائرات بدون طيار فقد يتم تشغيلها من موقع بعيد، كما تم استخدام الطائرات بدون طيار لتسليم الممنوعات مثل المخدرات والذخيرة والهواتف المحمولة إلى السجون عن طريق التحليق فوق الجدران، ففي مارس2019 تم اكتشاف طائرة بدون طيار مع مواد مهربة في منشأة تصحيح Collins Bay Institution في Ontario أونتاريو كندا، وقد تم تنفيذ تلك الجرائم في منشآت أخرى، ولم يتم الإعلان عن التدابير المضادة لمنع المزيد من الاستغلال وتكرار الأمر[3].

وفيما يتعلق بعمليات القرصنة يمكن تعديل الطائرات بدون طيار وإضافة مكونات إضافية لاستخدامها كأداة قرصنة متنقلة، فقد تمت إضافة كمبيوتر لوحي واحد مع اتصال G3 وحاقن حزمة Wi-Fi إلى طائرة Parrot AR Drone لإنشاء الروبوتات، تم اكتشاف شبكات Wi-Fi محمية بشكل ضعيف بواسطة الطائرات بدون طيار، وتم إرسال معلوماتهم إلى السحابة عبر شبكة G3 حيث تم كسرها وفي النهاية تم حقن الحزم في الشبكة، أيضاً في سنغافورة حيث أضاف الباحثون هاتفًا ذكيًا باعتباره حمولة الطائرة بدون طيار واستخدموه لاعتراض شبكات الطابعة، وبالتالي الوصول إلى المستندات المهمة في المساحات المكتبية [4].

(1) Orem drone pilot, girlfriend charged with voyeurism, [Online]. Available:https://www.kutv.com/news/local/orem-drone-pilot-girlfriend-chargedwith-voyeurism

(2) Criminal intent: FBI details how drones are being used for crime, [Online]. Available: https://www.techradar.com/news/criminal-intentfbi-details-how-drones-are-being-used-for-crime

(3) Correctional officials raise concern over drones smuggling contraband into Kingston-area prisons, [Online] Available : https://www.globalnews.ca/news/5074018/drones-smuggling-contraband-into-prisons-kingston/

(4) Hacking Wireless Printers With Phones on Drones, [Online]. Available: https://www.wired.com/2015/10/drones-robot-vacuums-can-spyoffice-printer/

ثالثاً: استخدام الطائرات المسيرة في العمليات الإرهابية:

فقد تم ما يُعرف بهجوم كراكاس بدون طيار، حيث تم تفجير طائرتين بدون طيار تحملان متفجرات بالقرب من Avenida Bolívar أفينيدا بوليفار في كراكاس فنزويلا حيث كان نيكولاس مادورو رئيس فنزويلا، يلقي خطابه أمام الحرس الوطني البوليفاري في 4 أغسطس 2018، وأفادت التقارير أن الطائرات بدون طيار هي DJI M600 نموذج محمل بالمتفجرات البلاستيكية C4 ومسحوق البنادق، وأسفر الحادث عن إصابة بعض جنود الحرس الوطني، وقد نشرت مجموعة إرهابية منشورات على وسائل التواصل الاجتماعي تزعم مسؤوليتها عن الهجوم[1]، كما استخدمت المنظمات الإرهابية مؤخرًا طائرات بدون طيار لتصوير هجماتهم وتدريبهم وعملياتهم باستخدام طائرات بدون طيار مزودة بكاميرات عالية الدقة (HD)، للدعاية عبر الانترنت في محاولة لتعزيز معنويات جهاديهم وحث المتعاطفين والداعمين في جميع أنحاء العالم للانضمام إليهم، أيضاً استخدامهم لتلك الطائرات بدون طيار لالتقاط لقطات حية (مثل الصور ومقاطع الفيديو) أثناء التخطيط لهجوم أو هجمات مستقبلية محتملة، وكذلك استخدامهم لتلك الطائرات لقصف أهداف حيوية للبنى التحتية[2].

رابعا: الهجوم السيبراني الواقع على الطائرات المسيرة:

أدى تطور تقنيات صناعة الطائرات بدون طيار إلى استخدام الدول لها في جميع المجالات الحيوية والاستراتيجية، واحتلت مكانة مهمة لدى مؤسسات ومرافق الأمن القومي للدول لاستخدامها في دعم الأنشطة والممارسات المتعلقة بسلطات واختصاصات تلك المرافق والمؤسسات، الأمر الذي جعلها هدفاً لأي هجوم سيبراني لما تحتويه تلك الطائرات من معلومات وبيانات حساسة، فضلاً عن تلك الطائرات قد تكون مرتبطة بمراكز القيادة والتحكم داخل مؤسسات ومرافق الأمن القومي للدول، ومن ثم فالاستيلاء عليها أو اختراقها قد يؤدي إلى أضرار أو تهديدات خطيرة للأمن القومي، ومن ثم أصبح وجود أي تهديد أو هجوم سيبراني على تلك الطائرات يُعد تهديداً أو هجوماً على أمن المعلومات القومي للدول.

(1) Venezuela's Maduro says drone blast was bid to kill him, blames Colombia, [Online]. Available:https://www.reuters.com/article/us-venezuela-politics/venezuelasmaduro-object-of-attack-but-fine-official-idUSKBN1KP0SA

(2) Jean-Paul Yaacoub, et al, op.cit.

بعض مظاهر الهجوم السيبراني الواقع على الطائرات المسيرة [1]:

- الهجوم السيبراني بانتحال نظام تحديد المواقع العالمي (GPS) فقد كشف تحليل التكوين ووحدات التحكم في الطيران لنماذج الطائرات بدون طيار، ذات الدوارات المتعددة، عن العديد من نقاط الضعف، التي قد تؤدي إلى انتحال نظام تحديد المواقع العالمي (GPS)، حيث لا تستطيع الطائرات بدون طيار الحصول على إشارات GPS شرعية و يُصدر المهاجم إشارة تشويش GPS تتداخل مع إشارات GPS، مما يتسبب في حدوث خلل في الطائرة بدون طيار لجهاز استقبال GPS ومن ثم يمكن بسهولة التقاط المعلومات أو تعديلها أو حقنها، فتُمكن هذه الثغرة الأمنية في رابط البيانات من الاعتراض والتحايل، مما يمنح المهاجمين سيطرة كاملة على الطائرة بدون طيار.
- الهجوم السيبراني بالتشويش على Wi-Fi حيث يمكن التشويش على تردد الطائرة بدون طيار وإغرائها للاتصال بشبكة Wi-Fi الخاصة بالهاكر، عن طريق تثبيت وتهيئة raspberry-pi لمثل هذه الوظيفة، ومن ثم يتم التحكم في الطائرة واستغلالها، وقد يؤدي الأمر إلى اختطافها.
- الهجوم السيبراني باستخدام رفض الخدمة (DoS) يتم تنفيذه عن طريق التحميل الزائد على جهاز أو شبكة الطائرة المسيرة بحركة مرور ضخمة أو طلبات أو حزم، مما يجعل الخدمة غير متاحة للمستخدم، ويترتب عليه منع الاتصال بين الطائرة والمشغل أو بينها وبين مراكز التحكم والقيادة، ومن ثم التحكم الكامل للمهاجم في الطائرة، وفي هذا النوع يصعب تحديد مصدر الهجوم.

(1) Bora Ly ORCID Icon &Romny Ly,"Cybersecurity in unmanned aerial vehicles (UAVs)", Journal of Cyber Security Technology, received 20 May 2020, Accepted 31 Oct 2020, Published online: 11 Nov 2020. https://www.tandfonline.com/doi/full/10.1080/23742917.2020.1846307

المبحث الثالث

استراتيجية تحقيق الأمن السيبراني لمرافق الأمن القومي

تمهيد:

سوف نتناول دراسة هذا المبحث من خلال مطلبين، المطلب الأول لدراسة محاور استراتيجية تحقيق الأمن السيبراني لمرافق الأمن القومي، والمطلب الثاني لدراسة استراتيجيات الدول لتحقيق الأمن السيبراني وخاصة الدول الرائدة في مجال تحقيق الأمن السيبراني، الولايات المتحدة الأمريكية، المملكة المتحدة، الصين، استراتيجية الاتحاد الأوربي، واستراتيجية دولة الإمارات العربية المتحدة.

المطلب الأول

محاور استراتيجية تحقيق الأمن السيبراني لمرافق الأمن القومي

المحور الأول
استخدام تقنية البلوكشين في تعزيز الأمن السيبراني لمرافق الأمن القومي[1]:

تُستخدم تقنية Blockchain بشكل خاص في تعزيز الأمن السيبراني لمرافق الأمن القومي، لخصائص تلك التقنية التي تتمثل في القدرة العالية على التكيف والموثوقية وإمكانية الوصول والكفاءة، ونتناول بعض هذه المجالات بالقدر المناسب لموضوع البحث على النحو التالي:[2]

1. تأمين الرسائل الخاصة (Securing Private Messaging) فيمكن استخدام تلك التقنية في تأمين وحماية الرسائل الخاصة لكونها تقنية عالية قائمة على خاصية التشفير، ومن ثم تشفير تلك الرسائل وحفظ وتأمين البيانات المتداولة، فيمكن لهذه التقنية إذا ما تم استخدامها جيداً أن تمنع الهجمات السيبرانية على البيانات والرسائل المتداولة، في المؤسسات والمرافق وبين الأفراد خاصة التي يتم تنفيذها ضد منصات التواصل الاجتماعي، فقد أسفرت الهجمات

(1) د. عماد الدين محمد كامل عبد الحميد، المرجع السابق، الجزء الثاني ص .26 - 28-27.

(2) Bora Ly ORCID Icon &Romny Ly,"Cybersecurity in unmanned aerial vehicles (UAVs)", Journal of Cyber Security Technology, received 20 May 2020, Accepted 31 Oct 2020, Published online: 11 Nov 2020. https://www.tandfonline.com/doi/full/10.1080/23742917.2020.1846307

السيبرانية على تلك المواقع عن العديد من الخروقات لملايين الحسابات ووصول المعلومات إلى الأيدي الخطأ.

2. تقنية البلوكشين تُضفي اللامركزية على وسيط التخزين Decentralizing Medium Storage أصبحت عمليات اختراق البيانات والسرقة سببًا رئيسيًا واضحًا لقلق المؤسسات والمرافق التي تستخدم الشكل المركزي لوسيط التخزين للوصول إلى البيانات المخزنة بالكامل، في هذه الأنظمة يستغل المهاجم ببساطة نقطة واحدة ضعيفة، ومن ثم تكون البيانات الحساسة والسرية في حوزة المجرم، وباستخدام Blockchain نستطيع حماية وتأمين الأسرار والمعلومات والبيانات من خلال نظام لامركزي للتخزين وللتداول لتلك المعلومات والأسرار والبيانات، والتي توفره هذه التقنية، ومن ثم يستحيل على المتسلل اختراق أنظمة التخزين.
3. حماية البلوكشين قطاع النقل الذكي (بدون سائق): منظومة النقل الذكي تعمل بدون سائق لقيادتها، حيث يتم التحكم في تحركاتها من خلال مركز تحكم مركزي عن بُعد، متصل بأجهزة استشعار بمرفق النقل، التي تقوم بنقل البيانات إلى مركز التحكم المركزي، فإذا ما تعرضت تلك الشبكات لهجوم سيبراني وتم اختراقها والوصول إليها، سوف يتم التحكم الكامل في وظائف مرفق النقل من قبل المعتدي، وما قد يترتب عليه من أضرار بالغة، وباستخدام تقنية Blockchain سيتم منع تلك الهجمات، لقدرتها على اللامركزية التي تقوم على توزيع مراكز ونقاط التحكم والسيطرة، فلا تجعلها في موقع واحد يمكن أن يتم التسلل إليه أو اختراقه.
4. تقنية البلوكشين وتعزيز مكافحة الإرهاب السيبراني[1]: تركز Blockchain وهي تقنية دفتر الأستاذ الموزع (DLT) على القدرة على تشفير الرسائل وحماية البيانات والمعلومات والأسرار، ومن ثم فقد تساعد في تأمين وحماية المرافق والمؤسسات وتمنع الهجمات السيبرانية، أياً كانت وسائلها قرصنة أو برامج الفدية أو تصيد، فتقنية Blockchain وتكنولوجيا دفتر الأستاذ الموزع هي دفاتر أستاذ لامركزية وغير مركزية تحافظ على الأصل الرقمي وتجعل تاريخ ذلك الأصل غير قابل للتغيير وشفافًا، كما تتيح الوصول الموزع إلى تلك الأصول الرقمية، والقدرة على نقل الأصول ونسخها، وإنشاء محفوظات وتغييرات مسجلة شفافة تحافظ على سلامة المستند، فأصبحت أداة قوية لمواجهة تحديات الأمن السيبراني وتوفير الأمن للمؤسسات العالمية.

(1) Olga Vorobyova, Julia Polyakova, Togliatti State University, Russian Federation, Olga Borzenkova, Samara State Social and Pedagogical University, Russian Federation, "Leading Opportunities for Fighting Cyberterrorism Using Blockchain Technology", Advances in Social Science, Education and Humanities Research, volume 441 6th International Conference on Social, economic, and academic leadership (ICSEAL-6-2019), Copyright © 2020 The Authors. Published by Atlantis Press SARL. file:///C:/Users/alfat/Downloads/1259409871)20%).pdf

5. تقنية البلوكشين وتعزيز الأمن السيبراني للقطاع المالي [1]:

في شهر مايو 2020 صدر عن البرلمان الأوربي دراسة تؤكد الدور الجوهري لتقنية Blockchain في حماية الأصول الرقمية للتجارة الدولية، لما تحققه تلك التقنية من تخزين آمن وقوي وموثق ومقاوم للتعديل، بقدرتها على تشفير البيانات والمعلومات والأسرار، ولطبيعتها اللامركزية التي تقوم على توزيع البنية التحتية ومراكز ونقاط التحكم والسيطرة، فلا تجعلها في موقع واحد أو جهة فاعلة واحدة لديها سيطرة كاملة عليها، وهذا يتناسب بشكل خاص مع الأنظمة البيئية للتجارة الدولية [2].

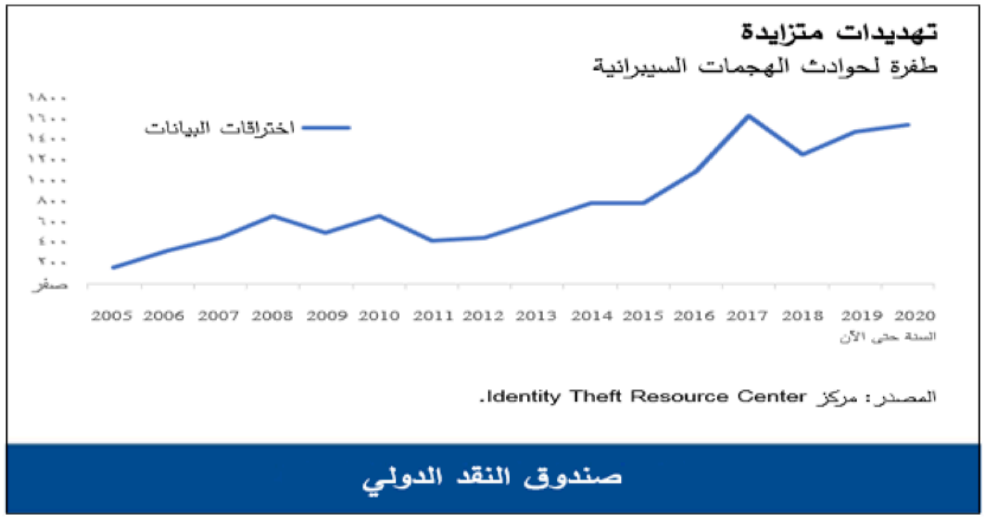
المحور الثاني
استراتيجية الأمن السيبراني للقطاع المالي للدول (صندوق النقد الدولي)[3]

تعتمد الصناعة المالية والمصرفية في أغلب دول العالم على تكنولوجيا الخدمات الرقمية، لذا فقد تضاعف عدد الهجمات السيبرانية على القطاع المالي، فنجاح أي هجوم سيبراني على مؤسسة مالية كبرى يمكن أن يكون له تداعيات خطيرة على النظام المالي للدولة، وما قد يصاحب ذلك من اضطراب وفقدان للثقة في تلك القطاعات الحيوية، فضلاً عن حبس السيولة وفشل المعاملات، وفقد القدرة على النفاذ إلى الودائع والمدفوعات، ومن ثم قد يضطر المستثمرون والمودعون إلى إلغاء حساباتهم والمطالبة بأموالهم أو غير ذلك من الخدمات والمنتجات التي يستخدمونها في العادة، ويوضح الشكل رقم (1) تلك التهديدات المتزايدة والطفرة الكبيرة لحوادث الهجمات السيبرانية على القطاع المالي لدول العالم حتى 2020.

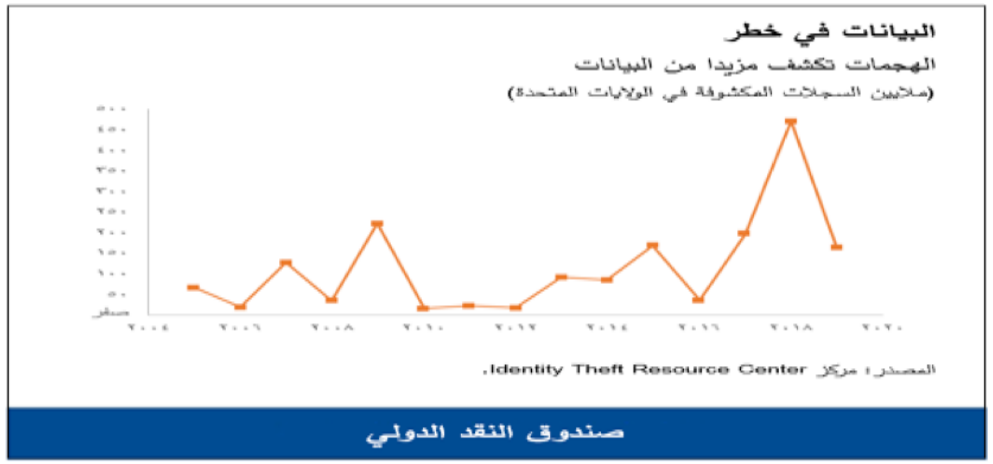
(1) Blockchain for supply chains and international trade, Study Panel for the Future of Science and Technology, EPRS | European Parliamentary Research Service, Scientific Foresight Unit (STOA), PE 641.544 – May 2020. https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641544/EPRS_STU(2020)641544_EN.pdf

(2) Ivica Nikolic´, Aashish Kolluri, School of Computing, NUS Singapore, Ilya Sergey, University College London United Kingdom, "Finding The Greedy, Prodigal, and Suicidal Contracts at Scale",14 Mar 2018. https://arxiv.org/pdf/1802.06038.pdf

(3) IMF staff discussion Note: Cyber Risk and Financial Stability: It's a Small World After All, Frank Adelman, Jennifer Elliott, Ibrahim Ergen, Tamas Gaidosch, Nigel Jenkinson, Tania Khiaonarong, Anastasiia Morozova, Nadine Schwarz, and Christopher Wilson, December 2020. file:///C:/Users/alfat/Downloads/SDNEA2020007.pdf
-لمزيد من التفاصيل راجع د. عماد الدين محمد كامل عبد الحميد، المرجع السابق ص 30-29-28.



فالهجمات السيبرانية عابرة للحدود بين مختلف دول العالم، ومن ثم أصبح الأمن السيبراني مصدر تهديد كبير للأمن القومي لمختلف دول العالم بمختلف أنواعه ومفرداته، فأصبحت البيانات والمعلومات وسجلات الأسرار في خطر، ويوضح مضمون كل ذلك الشكل رقم (2)



لذا فقد قام صندوق النقد الدولي ومن خلال مجموعة من خبرائه بوضع استراتيجية للأمن السيبراني للقطاع المالي للدول 2020، تقوم على عدة ركائز أولاً: التحديد الكمي للمخاطر وإعداد الخرائط السيبرانية (Preparing cyber maps and quantifying risks)، لأن من شأن ذلك تحسين القدرة على فهم المخاطر وتخفيف حدتها، وتركيز الاستجابة لمواجهتها، ثانياً: معالجة المخاطر

العابرة للحدود بالتنظيم والإشراف (Regulation and Supervision): فمن شأن ذلك أن يقلل من التكاليف ويبني منصة لتعاون أقوى ومشاركة للمعلومات، ومن ثم معالجة تلك المخاطر، ثالثاً: تحسين وظائف الاستجابة والتعافي (Response and Recovery): وذلك لصد الهجوم السيبراني أو الحد منه واستئناف العمليات بسرعة، رابعاً: تبادل المعلومات (Information Sharing): حول التهديدات والهجمات السيبرانية، خامساً: منع الهجوم السيبراني (Preventing Cyberattacks): من خلال تضافر الجهود الدولية لتعطيل وردع المهاجمين، من خلال إجراءات فعالة لمصادرة عائدات الجريمة ومقاضاة المجرمين، وتحقيق التعاون الوثيق بين أجهزة إنفاذ القانون بين مختلف دول العالم، سادساً: بناء وتنمية قدرات الأمن السيبراني (Capacity Development): فمن شأنه أن يؤدي إلى تعزيز الاستقرار المالي ودعم الشمول المالي، لذا فالبلدان منخفضة الدخل معرضة بشكل كبير للمخاطر السيبرانية.

المطلب الثاني

استراتيجيات الدول لتحقيق الأمن السيبراني لمواجهة الإرهاب السيبراني

وضعت أغلب دول العالم المتقدم خاصة التي أدرجت بنيتها التحتية عبر الفضاء السيبراني الأمن السيبراني على رأس أولوياتها باعتباره جزءاً من منظومة الأمن القومي لها، ومن ثم وضعت استراتيجيتها لمنظومة الأمن السيبراني لتأمينه وحمايته ضد أي تهديد أو اعتداء عليه، وسوف نتناول بعض هذه الاستراتيجيات لتكون دليلاً استرشادياً لعقد مقاربة بين الدول عند وضع استراتيجيتها، وبالقدر الذي يتناسب مع موضوع البحث ومتطلباته.

أولاً: استراتيجية الولايات المتحدة الأمريكية للأمن السيبراني [1]:

أ. نطاق الاستراتيجية (Scope of the strategy): في 15 مايو 2018 وضعت وزارة الأمن الداخلي استراتيجية الأمن السيبراني، وحددت نطاقها خلال السنوات الخمس القادمة 2023.

ب. ركائز الاستراتيجية وأهدافها: حددت الاستراتيجية خمس ركائز لتحقيق سبعة أهداف محددة عبر هذه الركائز الخمس، وذلك على النحو التالي: الركيزة الأولى تحديد المخاطر لتحقيق الهدف (1) تقييم مخاطر الأمن السيبراني المتطورة، وتحديد أولوياتها وإحاطة الجهات المختصة، الركيزة الثانية الحد من الضعف لتحقيق الهدف (2) وهو حماية نظم معلومات الحكومة الاتحادية، والعمل على تقليل نقاط ضعف الوكالات الفيدرالية لضمان تحقيقها لمستوى كافٍ من الأمن السيبراني، والهدف (3) وهو حماية البنية التحتية الحيوية، والمشاركة مع أصحاب المصلحة الرئيسيين لضمان إدارة مخاطر الأمن السيبراني الوطنية بشكل مناسب، الركيزة الثالثة الحد من التهديد لتحقيق الهدف (4) وهو منع الاستخدام الإجرامي للفضاء السيبراني وتعطيله، والعمل على تقليل التهديدات السيبرانية من خلال مواجهة المنظمات الإجرامية عبر الوطنية ومجرمي الإنترنت المتقدمين، الركيزة الرابعة تخفيف العواقب لتحقيق الهدف (5) وهو الاستجابة الفعالة للحوادث السيبرانية، والإقلال من عواقب الحوادث السيبرانية الخطيرة المحتملة من خلال جهود الاستجابة المنسقة.
الركيزة الخامسة تمكين نتائج الأمن السيبراني لتحقيق الهدف (6) وهو تعزيز أمن وموثوقية النظام البيئي السيبراني، ودعم السياسات والأنشطة التي تساعد إدارة مخاطر الأمن السيبراني العالمية، والهدف (7) وهو تحسين إدارة أنشطة الأمن السيبراني لوزارة الأمن الداخلي، والقيام بتنفيذ جهود إدارة الأمن السيبراني بطريقة متكاملة.

ج. المبادئ التوجيهية (Guiding Principles): لتعزيز مهمة وزارة الأمن الداخلي لتحقيق أهداف الأمن السيبراني تضمنت الاستراتيجية المبادئ التوجيهية وهي تحديد أولويات المخاطر خاصة للتركيز على المخاطر النظامية، وأكبر تهديدات الأمن السيبراني ونقاط الضعف التي يواجهها الشعب الأمريكي:

- فعالية التكلفة من خلال تقييم الجهود بشكل مستمر، وإعادة ترتيب الأولويات لضمان أفضل النتائج للاستثمارات التي يتم إجراؤها.
- الابتكار وخفة الحركة فيجب أن تكون وزارة الأمن الوطني قدوة يحتذى بها في البحث والتطوير والتكيف وتوظيف أحدث قدرات الأمن السيبراني لمواكبة التهديدات والتقنيات المتطورة.
- التعاون لتحقيق الأهداف في مجال الأمن السيبراني، يجب العمل بطريقة تعاونية عبر المكونات ومع شركاء اتحاديين وغير اتحاديين.
- النهج العالمي من خلال المشاركة والتعاون الدوليين لتحقيق الأهداف الوطنية للأمن السيبراني.
- الأسهم المتوازنة فيجب أن تدعم الجهود المبذولة للتخفيف من مخاطر الأمن السيبراني ودعم التجارة الدولية أيضاً، وتقوية الأمن الدولي، وتعزيز حرية التعبير والابتكار.
- القيم الوطنية فيجب أن تدعم وزارة الأمن الداخلي الخصوصية والحقوق المدنية

(1) U.S. Department of Homeland Security" Cybersecurity Strategy", May 15, 2018. https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf

والحريات المدنية وفقًا للقانون والسياسة المعمول بها، من خلال دمج حماية الخصوصية في برامج الأمن السيبراني.

ثانياً: استراتيجية الاتحاد الأوربي للأمن السيبراني [1]:

https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1379

موقع المفوضية الأوربية

أ. **نطاق الاستراتيجية:** بتاريخ 24 يوليو 2020 نشرت المفوضية على موقعها تقريراً يتضمن استراتيجية الاتحاد الأوربـي للأمن السيبراني، ولقد حددت نطاقها من حيث أن هذه الاستراتيجية توفر الآليات والتدابير والأدوات التي يجب تطويرها على مدار السنوات الخمس المقبلة 2025 لضمان الأمن في البيئة المادية والرقمية على مستوى الاتحاد الأوروبي.

ب. **ركائز الاستراتيجية:**

1. بيئة أمنية مستقبلية: من خلال قواعد جديدة لبنية تحتية مستقبلية مادية ورقمية متطورة وحيوية تتمتع بالحماية والاستعداد والمرونة لتحقيق الأمن السيبراني، ضمان حماية مادية أقوى للأماكن العامة وأنظمة الكشف المناسبة لصد الهجمات الإرهابية عليها، تحديد أولويات الأمن السيبراني الاستراتيجي وتوقع التهديدات الناشئة لضمان قدرة الاتحاد الأوروبي على الاستجابة لها، وحدة سيبرانية مشتركة كمنصة للتعاون المنظم والمنسق، بناء شراكات دولية قوية.
2. معالجة التهديدات المتطورة: من خلال التأكد من أن قواعد الاتحاد الأوروبي الحالية ضد مكافحة الجرائم السيبرانية مناسبة للغرض ومنفذة بشكل صحيح، التعاون الوثيق مع الشركاء الاستراتيجيين.
3. حماية الأوروبيين من الإرهاب والجريمة المنظمة: من خلال محاربة الإرهاب، اتخاذ خطوات لتعزيز تشريعات أمن الحدود والاستخدام الأفضل لقواعد البيانات الموجودة، جدول أعمال للتصدي للجريمة المنظمة بما في ذلك الاتجار بالبشر، أجندة وخطة عمل جديدة للاتحاد الأوروبي بشأن المخدرات ومكافحة تهريب الأسلحة النارية ومكافحة تهريب المهاجرين.
4. نظام بيئي أمني أوروبي قوي: بين الحكومات وسلطات إنفاذ القانون والشركات والمنظمات الاجتماعية، والعمل مع شركاء خارج الاتحاد الأوروبي لتأمين المعلومات والأدلة، وتعزيز التعاون مع الانتربول، إنشاء مركز ابتكار أوربي للأمن الداخلي، تنفيذ الاستراتيجية بتكامل تام وتماسك تحت مسؤولية الممثل الأعلى للاتحاد للشؤون الخارجية ونهج الأمان، على أن تصدر المفوضية تقارير منتظمة عن التقدم المحرز، وسيبقي البرلمان الأوروبي والمجلس وأصحاب المصلحة على اطلاع كامل ومشاركين في جميع الإجراءات ذات الصلة.

ثالثا: استراتيجية المملكة المتحدة للأمن السيبراني [1]:

نطاق الاستراتيجية: حددت الاستراتيجية نطاقها المكاني بأنها تغطي سائر أرجاء المملكة بكاملها، ومن حيث نطاقها الزمني فيكون من 2016 حتى 2021، ومن حيث نطاق عرضها للموضوعات، فهي تعرض تقييماً مُحدثاً للتهديدات الحالية والمتغيرة باستمرار، ومراجعة نقاط الضعف وتطورها خلال السنوات الخمس الماضية، ورؤية الحكومة لأمن المعلومات في عام 2021، والأهداف الرئيسية لتحقيق تلك الغاية.

الركائز: تحدد الاستراتيجية مجموعة موضوعية من الأهداف والإجراءات والمقاييس المحددة لثلاث ركائز مهمة:

1. الدفاع (Defend) ستعزز الحكومة دفاعات تكنولوجيا المعلومات الخاصة بها وتعمل مع الصناعة لضمان حماية الشبكات والبيانات والأنظمة في المملكة المتحدة من التهديدات الإلكترونية المتطورة، وأن لدى المملكة الوسائل للدفاع عن المملكة المتحدة ضد التهديدات

(1) Press release24 July 2020, Brussels, EU Security Union Strategy: connecting the dots in a new security ecosystem
https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1379

(1) HM Government, National Cyber Security Strategy 2016-2021, The RT Hon Philip Hammond MP, Chancellor of the Excheque, The RT Hon Ben Gummer MP, Minister for the Cabinet Office and Paymaster General.
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

السيبرانية المتطورة.

2. الردع (Deter) أن تصبح المملكة هدفاً صعباً لأي اعتداء في الفضاء الإلكتروني، وفي ذات الوقت لها القدرة على القيام بعمل هجومي في الفضاء الإلكتروني في حال الرغبة في ذلك.
3. التطوير (Develop) ستساعد الحكومة في تطوير القدرات الحيوية للمملكة المتحدة، بما في ذلك المهارات السيبرانية، فضلاً عن صناعة الأمن السيبراني، لمواكبة التهديدات السيبرانية.

رابعاً: استراتيجية الصين للأمن السيبراني:

قانون الأمن السيبراني الصيني 2017 [1]: الهدف من إصدار القانون يُعد قانون الأمن السيبراني هو الاستراتيجية الأولى التي وضعتها الصين للأمن السيبراني بتاريخ 1 يوليو 2017، ونطاق القانون يسري على إنشاء الشبكات وتشغيلها وصيانتها واستخدامها، والإشراف على الأمن السيبراني وإدارته داخل إقليم الدولة (م2).

د. **ركائز الاستراتيجية التي وضعها القانون:** بناء البنية التحتية للشبكة والتوصيل البيني

- تتخذ الدولة تدابير لمراقبة ومنع ومعالجة مخاطر وتهديدات الأمن السيبراني التي تنشأ داخل وخارج أراضي جمهورية الصين الشعبية.
- تحمي الدولة البنية التحتية الحيوية للمعلومات من الهجمات والاقتحام والتدخل والتدمير.
- تجري الدولة بنشاط التبادل والتعاون الدولي في مجالات حوكمة الفضاء السيبراني، والبحث وتطوير تقنيات الشبكات، وصياغة المعايير، ومكافحة الجرائم السيبرانية.
- تنفذ الدولة نظام حماية متعدد المستويات للأمن السيبراني.
- تدعم الدولة الشركات والمؤسسات التعليمية أو التدريبية، مثل مدارس التعليم العالي والمدارس المهنية، في تنفيذ التعليم والتدريب المتعلق بالأمن السيبراني.
- تنشئ الدولة نظام مراقبة الأمن السيبراني والإنذار المبكر والاتصال المعلوماتي.

هـ. **الاستراتيجية الدولية للتعاون في مجال الفضاء السيبراني[2]:** في سبتمبر 2020، أصدرت الصين الاستراتيجية الدولية للتعاون في مجال الفضاء السيبراني، حددت هذه الاستراتيجية أربعة مبادئ رئيسية السلام والسيادة والحكم المشترك والمنافع المشتركة، لتحقيق ستة أهداف

(1) Rogier Creemers, Paul Triolo, and Graham Webster," Cybersecurity Law of the People's Republic of China June 1, 2017. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/

(2) Ministry of Foreign Affairs and the Cyberspace Administration of China" International Strategy of Cooperation on Cyberspace", September 2020. file:///C:/Users/alfat/Downloads/China.pdf

محددة وهي الحفاظ على السيادة والأمن، تطوير نظام القواعد الدولية التي تحكم الفضاء السيبراني، تعزيز إدارة الإنترنت العادلة، حماية حقوق المواطنين، تعزيز التعاون، بناء منصة للتبادل الثقافي السيبراني.

و. **تدابير جديدة بشأن مراجعة الأمن السيبراني:** في أبريل 2020 أصدرت إدارة الفضاء السيبراني في الصين (CAC) و 11 وكالة حكومية أخرى بشكل مشترك تدابير جديدة بشأن مراجعة الأمن السيبراني [1] تنفيذاً لنص المادة 35 من قانون الأمن السيبراني الصيني (CSL")، التي تنص على أنه يتعين على مشغلي البنية التحتية للمعلومات الحرجة (CSL") الخضوع لمراجعة أمنية إذا كان شراء "منتجات وخدمات الشبكة" يتعلق بالأمن القومي الصيني،تهدف الإجراءات التي تم تطويرها على أساس قانون أمن الدولة وقانون الأمن السيبراني، إلى ضمان سلامة سلسلة التوريد للبنية التحتية للمعلومات الحيوية وضمان الأمن القومي، عندما يؤثر شراء منتجات وخدمات الشبكة من قبل مشغل البنية التحتية للمعلومات الحيوية ("المشغل") أو قد يؤثر على أمن الدولة، يجب على المشغل إخطار مكتب مراجعة الأمن السيبراني، الذي يخضع لـ CAC.

خامساً: الاستراتيجية الوطنية للأمن السيبراني لدولة الإمارات العربية المتحدة [2]:

الهدف من الإصدار: توفير بيئة سيبرانية آمنة وصلبة متطورة تُساعد على تمكين الأفراد من تحقيق طموحاتهم، وتمكن الشركات من التطور والنمو في بيئة آمنة مزدهرة، ودعم معايير الأمن السيبراني في الدولة عبر آليات ومحاور مختلفة، نطاق الاستراتيجية: تم إصدارها في 2019 من قبل الهيئة الاتحادية لتنظيم قطاع الاتصالات، فهي الجهة المختصة في قطاع الاتصالات وتكنولوجيا المعلومات، والمسؤولة عن التحول السيبراني والذكي في الدولة، ويسري تطبيق هذه الاستراتيجية لمدة ثلاث سنوات، ومراجعتها وفق مستجدات الأمن السيبراني.

ركائز الاستراتيجية: تضم الاستراتيجية منظومة متكاملة للأمن السيبراني، قائمة على خمس ركائز

(1) Yan Luo and Zhijing Yu"China Issues New Measures on Cybersecurity Review of Network Products and Services,27-4-2020. https://www.insideprivacy.com/international/china/china-issues-new-measures-on-cybersecurity-review-of-network-products-and-services/ --Privacy & Information Security Law Blog, Global Privacy and Cybersecurity Law Updates and Analysis, "China Issued Measures for Cybersecurity Review" Posted on April 29, 2020.

(2) هيئة تنظيم الاتصالات – دولة الامارات العربية المتحدة https://www.tra.gov.ae/userfiles/assets/IJP6zPkDr3.pdf

و60 مبادرة، الركيزة الأولى إطار قانوني وتنظيمي شامل للأمن السيبراني: لمكافحة جميع أنواع الجرائم السيبرانية، وبناء إطار تنظيمي لحماية التقنيات الحالية والناشئة، ووضع أنظمة داعمة لتمكين الشركات الصغيرة والمتوسطة وحمايتها من التهديدات السيبرانية، الركيزة الثانية منظومة حيوية للأمن السيبراني من خلال: الاستفادة من سوق الأمن السيبراني في الدولة والذي تصل قيمته إلى 8,1 مليار درهم، والمشاركة بفعالية في سوق الأمن السيبراني في منطقة الشرق الأوسط وشمال أفريقيا، تطوير قدرات أكثر من 40,000 من المتخصصين في الأمن السيبراني، وتشجيع المهنيين والطلبة على الانخراط في المجال، بناء القدرات وتطوير منظومة متكاملة في مجال التدريب في الأمن السيبراني، زيادة الوعي بالأمن السيبراني والمخاطر المتعلقة بالإنترنت، وتشجيع المؤسسات على إطلاق برامج حول الأمن السيبراني، ودعم الأبحاث الخلاقة في المؤسسات الأكاديمية، الركيزة الثالثة خطة فعالة للاستجابة للحوادث السيبرانية من خلال: تنظيم آلية الكشف عن حوادث الأمن السيبراني والإبلاغ عتها، إنشاء منهجية موحدة لتقييم درجة خطورة الحوادث لتوفير الدعم المناسب، بناء قدرات وطنية على مستوى عالمي للاستجابة لجميع أنواع الحوادث السيبرانية، الركيزة الرابعة حماية الأصول الحيوية لدولة الإمارات في تسعة قطاعات: هي الطاقة، الاتصالات وتقنية المعلومات، القطاع الحكومي، الكهرباء والمياه، القطاع المالي والتأمين، خدمات الطوارئ، المواصلات، الغذاء والزراعة، الخدمات الصحية الركيزة الخامسة دعم عمل منظومة الأمن السيبراني: من خلال عقد شراكات على المستوى المحلى والعالمي، تساهم في تحقيق أهداف وطموحات الدولة، ويشمل القطاع العام والخاص، المؤسسات الأكاديمية، الجمعيات والمنظمات الدولية.

الخاتمة

أولاً: النتائج:

1. ارتكزت البنى التحتية على الفضاء السيبراني، فأصبحت حمايتها من أولويات الأمن القومي، وقوة جذب للاعتداء عليها بالإرهاب السيبراني أو الحروب السيبرانية، لأسباب وردت في البحث.
2. إن هناك تداخلاً وخلطاً بين مفهوم الإرهاب السيبراني والحروب السيبرانية بين مختلف دول العالم، ترتب عليه تحديات قانونية في بسط الحماية المطلوبة.
3. الهجمات السيبرانية والاعتداء على البنى التحتية يُمثلان القاسم المشترك بين الإرهاب السيبراني والحروب السيبراني.
4. يُعرّف الباحث الإرهاب السيبراني بأنه هجوم سيبراني الغرض منه تهديد الحكومات أو العدوان عليها، أو الإخلال بالنظام العام أو تعريض سلامة أو مصالح أو أمن المجتمع وأفراده للخطر، سعياً لتحقيق أهداف سياسية أو عقائدية أو أيدولوجية.
5. كما-يُعرّف الباحث الحروب السيبرانية: بأنها هجوم سيبراني تقوم به دولة أو أحد من يعملون لمصلحتها على مرافق ومؤسسات البنى التحتية المدرجة عبر الفضاء السيبراني لدولة أخرى، يترتب عليه وقوع أضرار بالأمن القومي بمفهومه الشامل للدولة المعتدى عليها.
6. تزايدت وتيرة الهجمات السيبرانية وتطورت تقنياتها في الفترة الأخيرة وفقاً لإحصائيات مؤسسات دولية، للأسباب التي وردت في متن البحث، الموثقة بحوادث الهجوم من 2019 إلى 2021.
7. فرض الإرهاب السيبراني العديد من التحديات القانونية والأمنية سواء تمثل في صعوبة ضبط تلك الجرائم وملاحقة مرتكبيها لعدم القدرة على تحديد مصدر الهجوم، أو لضعف منظومة الأمن السيبراني لدى مختلف الدول، أو لضعف البنى التحتية لأجهزة العدالة الجنائية الرقمية.
8. تطور مفهوم الأمن القومي بعد إدراج مرافق البنى التحتية عبر الفضاء السيبراني، ومن ثم قد ارتبط بمنظومة الأمن السيبراني لدى الدول، ومدى قوتها وتطورها لحماية تلك المرافق، فأصبح ضعف منظومة الأمن السيبراني يهدد الأمن القومي للدول، وتُعد هجمات الإرهاب السيبراني على مرافق الأمن القومي 2020-2021 التي أوردها الباحث في متن بحثه خير دليل على ذلك.
9. أدى تعدد وتنوع الطائرات المسيرة وتطور تقنياتها إلى تهديد خطير للأمن القومي للدول.
10. أصبح استخدام الطائرات المسيرة في عمليات التجسس والقرصنة والتهريب والعمليات الإرهابية يُمثل تحديات قانونية وأمنية أمام أغلب دول العالم ومؤسساته الدولية.

11. تطور تقنيات صناعة الطائرات المسيرة أدى إلى استراتيجية استخدامها من قبل مؤسسات ومرافق الأمن القومي للدول، مما ترتب علية أن أصبحت هدفاً لأي هجوم سيبراني لما تحتويه تلك الطائرات من معلومات وبيانات حساسة قد تكون مرتبطة بمرافق ومؤسسات الأمن القومي، ولقد بين الباحث في متن بحثه بعض مظاهر الهجوم السيبراني الواقع على الطائرات المسيرة.
12. أصبحت تقنية البلوكشين أداة قوية لتعزيز الأمن السيبراني لمرافق الأمن القومي.
13. وضع صندوق النقد الدولي استراتيجية لتحقيق الأمن السيبراني للقطاع المالي للدول 2020، باعتباره أحد أولويات الأمن القومي، لحمايته من الإرهاب السيبراني، وردت في متن البحث.
14. أورد الباحث استراتيجيات دول العالم المتقدم لتحقيق الأمن السيبراني لمواجهة الإرهاب السيبراني، الولايات المتحدة الأمريكية، الصين، الاتحاد الأوربي، المملكة المتحدة، دولة الإمارات.

ثانياً: استراتيجية الباحث لتحقيق الأمن السيبراني لمواجهة الإرهاب السيبراني[1]:

المحور الأول: الأمن المادي هو خط الدفاع الأول: يرى الباحث وبناء على ما ورد من تقارير دولية لخبراء الأمن السيبراني أنه لا يمكن لأي دولة أو مؤسسة على مستوى العالم أن تحقق الأمن السيبراني بنسبة 100%، وكل ما يمكن عمله هو تقليل مخاطر التهديد والهجمات السيبرانية بشكل كبير إلى المستوى الذي يسمح بالاستمرار في الاستفادة من الفرص الهائلة التي توفرها التكنولوجيا الرقمية، لأننا في عصر صراع التقنيات، فكل ثانية هناك تقنية جديدة، تخترق وتقوض ما سبقها من تقنيات، لذا نرى أن خط الدفاع الأول لحماية منظومة الأمن السيبراني هو توفير وتحقيق الأمن المادي لتلك المنظومة، فبدون توفير وتحقيق الأمن المادي لا يمكن الحديث عن استراتيجية فاعلة لتحقيق الأمن السيبراني.

فالأمن المادي هو حماية الأجهزة الفعلية ومكونات الشبكات التي تخزن موارد المعلومات وتنقلها، من خلال اتخاذ منظمة الأمن السيبراني مجموعة من التدابير، أولها تحديد جميع الموارد المعرضة للخطر واتخاذ التدابير لضمان عدم إمكانية الوصول إليها، أو العبث بها أو سرقتها، من خلال تعزيز الأبواب المغلقة لضمان عدم الوصول إلى تلك الموارد المعرضة للخطر، ولتأمين أصول المعلومات

(1) د. عماد الدين محمد كامل عبد الحميد، المرجع السابق الجزء الثاني ص 31-30.

عالية القيمة، فضلاً عن ضرورة متابعة مراقبة تلك الأصول من خلال استخدام الكاميرات الأمنية والوسائل الأخرى للكشف عن الوصول غير المصرح به إلى المواقع المادية حيث توجد، واتخاذ تدابير لتأمين المعدات والأجهزة لعدم فتحها والحصول على مدخرات معلوماتها، والاحتفاظ بخوادم المؤسسة وغيرها من المعدات عالية القيمة في غرفة يتم مراقبتها من أجل درجة الحرارة والرطوبة وتدفق الهواء لحمايتها، وعدم السماح لموظفي المؤسسة بحيازة أجهزة الكمبيوتر المحمولة خارج المؤسسة، لعدم تعرضها للسرقة، أو تأمينهم في حال ذلك لحماية البيانات المدرجة

المحور الثاني: تحديث وتطوير منظومة الأمن السيبراني وتنمية وتدريب قدرات القائمين عليها والاعتماد على الكفاءات الوطنية وانتقاؤها للعمل في المناطق والمواقع الحرجة في تلك المنظومة.

المحور الثالث: مراجعة دورية لمنظومة الأمن السيبراني نوصي بضرورة اتخاذ تدابير جديدة بشأن مراجعة دورية لمنظومة الأمن السيبراني، للبُعد الدولي المرتبط بأصول التشفير، ولكونها عابرة للحدود في تطبيقاتها وبنيتها التحتية، فضلاً عن سرعة تطور تلك الأصول المشفَرة وتعقيدها، كما يجب أن يكون هناك تقييم مستمر للتشريعات الصادرة للتحقق مما إذا كان يمكن تطبيقها بشكل فعال على هذا النوع من الأصول أو إذا كانت هناك حاجة إلى تعديلات أو إرشادات.

المحور الرابع: تعزيز وتطوير أجهزة العدالة الجنائية في التحقيقات الرقمية: للتأكد من أن لديهم الأدوات والتقنيات والمهارات المناسبة، الذكاء الاصطناعي، البيانات الضخمة، الحوسبة عالية الأداء في السياسة الأمنية، كل ذلك يُمثل أولية جوهرية لتحقيق الأمن السيبراني.

المحور الخامس: ضرورة الاستثمار في مجال الأمن السيبراني، وعقد شراكات دولية مع الدول الرائدة والمتطورة في هذا المجال لمشاركة معلومات التهديد السيبراني، لتحديد معالم التطور العالمي للفضاء الإلكتروني، ولإنشاء مراكز جديدة للابتكار الإلكتروني، لإيجاد نظام كامل لحماية الأمن السيبراني، ولرفع القدرة على حماية الأمن السيبراني.

المحور السادس: نحذر من شراء منظومات الحماية الخاصة بالأمن السيبراني: لما قد تتضمنه تلك المنظومات من مخاطر على الأمن القومي بمفهومه الشامل، فقد تتضمن تلك المنظومة تقنيات مشفرة مجهولة للتجسس أو إتلاف أو العبث في بيانات أو معلومات المؤسسة المستضيفة لتك المنظومة، أو الحصول على هامش بسيط لا يذكر ولا يُلحظ من تداول الأصول المالية في المؤسسات المصرفية أو المالية المستضيفة لتلك المنظومة، ولتلافي تلك المخاطر يجب تجربة منظومة حماية الأمن السيبراني المستوردة في قطاعات غير حيوية أو قطاعات محاكاة تدريبية، لتجربتها وتدريب الكوادر الوطنية عليها وفك شفراتها وفقه جوهرها، ثم بعد ذلك نقلها إلى القطاعات الحيوية، مع إدارتها وتشغيلها بكفاءات وطنية عالية ومدربة.

المحور السابع: تصنيع وإنتاج الطائرة المسيرة وتقنياتها والتطبيقات الذكية لمراقبتها (وطنياً):

يحذر الباحث من شراء التطبيقات الذكية الخاصة بتحقيق الأمن السيبراني في مجال الطائرات المسيرة، نظراً لما قد تتضمنه من تقنيات تجسس متطورة ومجهولة داخل تلك التطبيقات، تستطيع التقاط البيانات والترددات وتحليلها، ورسم الخرائط ثلاثية الأبعاد للمواقع الاستراتيجية، وإرسال كل التقارير إلى الطرف الآخر، لذا فيوصي الباحث بصناعة وإنتاج الطائرة المسيرة وتقنياتها محلياً مع توفير الاعتمادات المالية والكوادر المدربة للنهوض بتلك الصناعات، ومن ثم يحذر الباحث من عدم شراء أو استيراد تلك المنظومة، وخير دليل على ذلك مراجعة الولايات المتحدة الأمريكية منظومة استيراد أو شراء تلك المنظومات من دولة الصين لاكتشافها تحقق المخاطر السابقة.

المحور الثامن توصيات خاصة:

1. كما يوصي الباحث بضرورة عقد اتفاقية دولية موحدة تحت منظمة الأمم المتحدة تتضمن التنظيم القانوني الموحد لصناعة وإنتاج واستخدام الطائرات المسيرة، لمواجهة التحديات القانونية والأمنية التي تفرضها تلك الطائرات، خاصة فيما يتعلق بحماية منظومة الأمن القومي للدول، والسعي لانضمام الدول إليها وتعديل جميع تشريعاتها وفق ذلك التنظيم القانوني الموحد للاتفاقية.
2. نوصي المشرع الإماراتي بإصدار قانون اتحادي موحد يتناول تنظيم صناعة وإنتاج واستخدام الطائرات المسيرة، لمخاطرها على الأمن القومي.
3. إنشاء جامعة متخصصة في الأمن السيبراني، لتكون نواة لبنية تحتية متطورة من الكفاءات الوطنية القادرة على حماية المنشآت الحيوية والاستراتيجية للدولة، وإنشاء إدارات خاصة بالأمن السيبراني في جميع مؤسسات وهيئات ووزارات للدولة لنشر ثقافة الأمن السيبراني وأخلاقيات التعامل مع الانترنت.

قائمة المراجع:

1. Algirde Pipikaite, et, al "These are the top cybersecurity challenges of 2021", World Economic Forum, 21 Jan 2021.
2. Anjali C. Das,"U.S. Government Warns Companies of Legal Risk for Paying Ransom to Cybercriminals", The National Law Review, Volume XI, Number 83. March 24, 2021.
3. Bora Ly ORCID Icon &Romny Ly,"Cybersecurity in unmanned aerial vehicles (UAVs)", Journal of Cyber Security Technology, received 20 May 2020, Accepted 31 Oct 2020, Published online: 11 Nov 2020.
4. Blockchain for supply chains and international trade, Study Panel for the Future of Science and Technology, EPRS | European Parliamentary Research Service, Scientific Foresight Unit (STOA), PE 641.544 – May 2020.
5. Christopher O'Brien," What is cyber-terrorism, and is it a threat to U.S. national security?" Small wars journal, Thu, 11/04/2021.
6. Clay Wilson, Cong. Research Serv., RL32114, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress 4 (2003) (Quoting Ron Dick, then Director of the NIPC).
7. CYBERDEFENSE REPORT, Japan's National Cybersecurity and Defense Posture, Policy and Organizations, Zürich, September 2020, Cyber Defense Project (CDP) Center for Security Studies (CSS)، ETH Zürich
8. Congressional Research Service, "Defense Primer: Electronic Warfare", Updated October 29, 2020. https://fas.org/sgp/crs/natsec/IF11118.pdf
9. Center for Strategic &International Studies, (CSIS), Significant Cyber Incidents
10. Criminal intent: FBI details how drones are being used for crime, [Online]. Available: https://www.techradar.com/news/criminal-intentfbi-details-how-drones-are-being-used-for-crime
11. Correctional officials raise concern over drones smuggling contraband into Kingston-area prisons, [Online] Available : https://www.globalnews.ca/

news/5074018/drones-smuggling-contraband-into-prisons-kingston/
12. David E. Sanger, "Russian Hackers Broke Into Federal Agencies, U.S. Officials "Dec. 13, 2020, Updated Feb. 9, 2021. https://www.csoonline.com/article/3237324/what-is-a-cyber-attack-recent-examples-show-disturbing-trends.html
13. Denning, Dorothy, E," Cyber terrorism"، Global Dialogue, Aug 2000, p01.
14. Dave Wallen," Types of Cyber Attacks: A Closer Look at Common Threats", October 6, 2020.
15. Drones, What Is A Drone? What Are Uses For Drones? April 2021. https://builtin.com/drones
16. Hacking Wireless Printers With Phones on Drones, [Online]. Available: https://www.wired.com/2015/10/drones-robot-vacuums-can-spyoffice-printer/
17. HM Government, National Cyber Security Strategy 2016-2021, The RT Hon Philip Hammond MP, Chancellor of the Excheque, The RT Hon Ben Gummer MP, Minister for the Cabinet Office and Paymaster General.
18. ITU/BDT Cyber Security Programme, Global Cybersecurity Index (GCI), Guidelines for Member States, Version 0.9.04 September 2019.
19. ICAO, "UNITING AVIATION "A United Nations Specialized Agency. https://www.icao.int/about-icao/Pages/default.aspx
20. Ivica Nikolic´, Aashish Kolluri, School of Computing, NUS Singapore, Ilya Sergey, University College London United Kingdom, "Finding The Greedy, Prodigal, and Suicidal Contracts at Scale",14 Mar 2018.
21. IMF staff discussion Note: Cyber Risk and Financial Stability: It's a Small World After All, Frank Adelman, Jennifer Elliott, Ibrahim Ergen, Tamas Gaidosch, Nigel Jenkinson, Tania Khiaonarong, Anastasiia Morozova, Nadine Schwarz, and Christopher Wilson, December 2020. file:///C:/Users/alfat/Downloads/SDNEA2020007.pdf
22. Jonalan Brickey , 'Defining Cyberterrorism: Capturing a Broad Range of Activities in Cyberspace', CTC Sentinel, August 2012, Vol. 5, No. 8, p. 6. https://ctc.usma.edu/wp-content/uploads/2012/08/CTCSentinel-Vol5Iss81.pdf
23. James A. Lewis," Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats, Center for Strategic and International Studies, December 2002.
24. Josh Fruhlinger, "What is a cyber-attack? Recent examples show disturbing trends"FEB 27, 2020.
25. Jan Wolfe and Brendan Pierson," Suspected Russian Hack of U.S. Government: Espionage or Act of War?" insurance journal, December 21, 2020.
26. John Bull, 'You Hacked: Cyber-Security and the Railways', London Reconnections, May 12, 2017.
27. (27) John Leyden, 'Polish teen derails tram after hacking tram network', The Register, 11 Jan 2008.
28. (28) Jean-Paul Yaacoub, et, al," Security analysis of drones' systems: Attacks, limitations, and recommendations", US National Library of Medicine National Institutes of Health,2020 Sep. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7206421/
29. Kelly A. Gable, Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent, 43 Vand. J. Transnat'l L. 57, 62 (2010).
30. Linn F. Freedman," Ransomware Attacks Predicted to Occur Every 11 Seconds in 2021 with a Cost of $20 Billion", The National Law Review, Volume XI, Number 82. March 23, 2021.
31. Mary K. Pratt," cyber-attack. January 2021. https://searchsecurity.techtarget.com/definition/cyber-attack#:~:text=A20%cyber20%attack20%is20%any,data20%held20%within20%these20%systems
32. Megan Hardiman," Corona Viruses and Computer Viruses: It's Time for a Cyber Health Check-Up", The National Law Review, Volume XI, Number 82. March 23, 2021.
33. Ministry of Foreign Affairs and the Cyberspace Administration of China"

International Strategy of Cooperation on Cyberspace", September 2020. file:///C:/Users/alfat/Downloads/China.pdf

34. Dr. Nick Oberheiden. "Defending Against National Security Threats," The National Law Review, Volume XI, Number 82. March 23, 2021.
35. Olga Vorobyova, Julia Polyakova, Togliatti State University, Russian Federation, Olga Borzenkova, Samara State Social and Pedagogical University, Russian Federation, "Leading Opportunities for Fighting Cyberterrorism Using Blockchain Technology", Advances in Social Science, Education and Humanities Research, volume 441 6th International Conference on Social, economic, and academic leadership (ICSEAL-6-2019), Copyright © 2020 The Authors. Published by Atlantis Press SARL.
36. Orem drone pilot, girlfriend charged with voyeurism, [Online]. Available:https://www.kutv.com/news/local/orem-drone-pilot-girlfriend-chargedwith-voyeurism
37. Press release24 July 2020, Brussels, EU Security Union Strategy: connecting the dots in a new security ecosystem. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1379
38. Richard A. Clarke & Robert knake, Cyber War: The Next Threat to National Security and What to Do About It, HarperCollins, 2010, p:6.
39. (39) Rogier Creemers, Paul Triolo, and Graham Webster," Cybersecurity Law of the People's Republic of China June 1, 2017. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/
40. S. Sagiroglu, "Cyber security and defence: importance, definitions and precautions," in Cyber Security and Defence—Awareness and Deterrence, vol. 1, pp. 21–45, Grafiker Press, Ankara, Turkey, 2018.View at: Google Scholar
41. Susan W. Brenner, "At Light Speed" - Attribution and Response to Cybercrime/Terrorism/Warfare, 97 J. Crim. L. & Criminology 397, 386 (2007)
42. Stefan Soesanto, "Cyber Terrorism. Why it exists, why it doesn't, and why it will", ARI 47/2020 - 17/4/2020. http://www.realinstitutoelcano.org/wps/portal/rielcano_en/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_in/zonas_in/ari47-2020-soesanto-cyber-terrorism-why-it-exists-why-it-doesnt-and-why-it-will
43. Steve Ranger," What is cyberwar? Everything you need to know about the frightening future of digital conflict", December 4, 2018.
44. The Federal Aviation Administration (FAA). Nov 6, 2020 https://www.faa.gov/uas/espanol/glosario/
45. (45) U.S. Department of Homeland Security" Cybersecurity Strategy", May 15, 2018. https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf
46. UNTERM, "Cyber warfare" warfare, https://unterm.un.org/UNTERM/display/Record/UNHQ/NA/c263537.View at: Google Scholar
47. Vinay Chamola, a, b Pavan Kotesh, et al" A Comprehensive Review of Unmanned Aerial Vehicle Attacks and Neutralization Techniques", US National Library of Medicine, National Institutes of Health, Search database,, 2021 Feb 1. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7547616/
48. Venezuela's Maduro says drone blast was bid to kill him, blames Colombia, [Online]. Available:https://www.reuters.com/article/us-venezuela-politics/venezuelasmaduro-object-of-attack-but-fine-official-idUSKBN1KP0SA
49. William L. Tafoya, Ph.D., Cyber Terror, FBI Law Enforcement Bulletin, Nov. 2011, https://www.fbi.gov/stats-services/publications/law -enforcement-bulletin/November-2011/cyber-terror.
50. Yan Luo and Zhijing Yu"China Issues New Measures on Cybersecurity Review of Network Products and Services,27-4-2020. https://www.insideprivacy.com/international/china/china-issues-new-measures-on-cybersecurity-review-of-network-products-and-services/

دور الذكاء الاصطناعي في تحقيق العدالة الجنائية (التشريع الإماراتي نموذجًا)

بقلم

الدكتور/ محمد عبد الله العوَّا

الخبير القانوني بالهيئة الاتحادية للضرائب
أستاذ القانون الجنائي المساعد
محامٍ لدى محكمة النقض والإدارية والدستورية العليا المصرية

مجلة علمية محكمة | العدد (15) | السنة العاشرة | ذو القعدة 1443 هـ | يونيو 2022م

دور الذكاء الاصطناعي في تحقيق العدالة الجنائية (التشريع الإماراتي نموذجًا)

الدكتور/ محمد عبد الله العوّا

الخبير القانوني بالهيئة الاتحادية للضرائب

أستاذ القانون الجنائي المساعد

محامٍ لدى محكمة النقض والإدارية والدستورية العليا المصرية

ملخص:

يجب أن نعترف بأن الذكاء الاصطناعي أصبح لديه القدرة على أن يكون جزءاً دائماً من جميع مراحل الدعوى الجنائية، وباتت الخوارزميات أداة جديدة لإنفاذ القانون، فأصبحت تطبيقاته تشكل عاملًا مهماً في جمع الأدلة الجنائية من خلال التنبؤ بالجرائم أو المساعدة في تقييم مخاطر العودة إلى الإجرام أو مواجهة الاحتيال المصرفي وغيره من الجرائم، فضلًا عن دوره في الكشف عن المشتبه بهم والتعرف على صور المجني عليهم، ومساعدته في معالجة أدلة الحمض النووي، بل وكشف الطلقات النارية.

كما برز دور الذكاء الاصطناعي في أنظمة المحاكمات الجنائية من خلال المساعدة في دعم اتخاذ القرار القضائي عن طريق أتمتة السوابق القضائية، وتقنيات سماع أطراف وشهود الدعوى الجنائية من معاقي السمع أو النطق، فضلًا عن المساعدة في سرعة الفصل في القضايا الجنائية وتقدير التعويضات الناشئة عن الجرائم، بالإضافة إلى تطوير السياسات العقابية وتوكيد اليقين القانوني.

الكلمات الدالة: المحاكمة – الجرائم – العقاب - أتمتة – تنميط – السوابق.

Abstract:

We must admit that artificial intelligence has the ability to be a permanent part of all stages of a criminal case, and algorithms have become a new tool for law enforcement, and its applications have become an important factor in collecting forensic evidence by predicting crimes or helping assess the risks of returning to crime or confronting Banking fraud and other crimes, in addition to its role in uncovering suspects, identifying photos of the victims, and assisting them in processing DNA evidence, and even detecting bullets.

The role of artificial intelligence has also emerged in criminal trial systems by helping to support judicial decision-making by automating judicial precedents, and techniques for hearing parties and witnesses of a criminal case who are hearing or speech impaired, as well as assisting in speeding up the adjudication of criminal cases and estimating compensation arising from crimes. In addition to the development of punitive policies and legal certainty.

Key words: Trial - Crimes - Punishment - Automation – profiling - Precedents.

مقدمة:

قد تنظر الأجيال القادمة إلى زماننا وتصفه بأنه كان زمن تغيّرات هائلة، ففي بضعة عقود تحوّلنا من مجتمع يعتمد على الآلات إلى الاعتماد على المعلومات، وفيما واصل عصر المعلومات النضوج وجد المجتمع نفسه مرغمًا على التمتع بألفةٍ جديدةٍ مع النظم الخوارزمية والقائمة على البيانات، وظهرت الأدوات المساعدة على صنع القرار والتي تعتمد على إجراءات تعلّم خوارزمية (بما فيها الذكاء الاصطناعي) [1]، كما مرت الإنسانية بالعديد من المتغيرات المتلاحقة، حتى أن جوانب حياتنا يتم رصدها وتخزينها واستخدامها بل وإساءة استخدامها رقميًّا، فمثلًا جميع من يحمل هاتفًا ذكيًّا يخلق مسارًا رقميًّا يؤدّي مباشرة إلى معرفة المكان الذي يوجد فيه[2]، ومع التطور في وسائل مكافحة الجريمة سعت أجهزة إنفاذ القانون لاستخدام وسائل التكنولوجيا المتاحة لملاحقة الجناة، وحينما ظهرت رويدًا تقنيات الذكاء الاصطناعي Artificial Intelligence (AI) أعلنت قدرة (الآلة) على محاكاة السلوك البشري الذكي وعملياته الإدراكية في التعرف على الأشياء عبر ملايين المعطيات والأوامر المُعدة سلفًا لوضع الحلول للمشكلات ومعالجة المعرفة والنظم الخبيرة، بما مهد الطريق لمستقبل واعد في نظام العدالة الجنائية من جهة توقع ومنع ارتكاب الجرائم، وسرعة إنجاز مراحل جمع الأدلة وصولاً للمحاكمات والترضية القضائية من جهة، وتحقيقًا للردع الخاص والعام من جهة أخرى عبر تحليل الروابط بين الأدلة المتاحة على ارتكاب الجريمة كنظام التعرف التلقائي على ملامح الوجه وتحليل الحمض النووي DNA، واستخراج المعلومات ذات الصلة بالتاريخ الجنائي وسجلات السوابق الجنائية لتقديم قوائم المرشحين لارتكاب جرائم معينة مثل القتل أو السطو أو الخطف، وهو ما يجعل النظام القانوني أكثر كفاءة في تحقيق العدالة الجنائية.

ويهتم علم الذكاء الاصطناعي بالعمليات المعرفية التي يستخدمها الإنسان في تأدية الأعمال التي نعدها ذكية، فقد تكون مسألة رياضية أو القيام بتشخيص طبي، أو الاستدلال على طريق للانتقال من مكان إلى آخر، حيث يبدأ الباحث في هذا العلم عمله أولًا باختيار أحد الأنشطة المتفق على أنها ذكية، ثم يضع بعض الفروض عما يستخدمه الإنسان لدى قيامه بهذا النشاط من معلومات واستدلالات، ثم يدخل هذه في برنامج للحاسب الآلي ويقوم بملاحظة سلوكه ما قد يؤدي إلى اكتشاف أوجه قصور، فيعمل على إدخال تعديلات وتطوير في البرنامج بما يؤدي إلى سلوك

(1) Osonde A. Osoba & William Welser IV - The Risks of Artificial Intelligence to Security and the Future of Work - PE-237/1-RC (2017) – Available on line at www.rand.org – P.1.

(2) ميشيل باشيليت "مفوّضة الأمم المتّحدة السامية لحقوق الإنسان" - حقوق الإنسان في العصر الرقمي – متاح في 2021/01/06 على موقع: www.ohchr.org/AR/NewsEvents

مختلف وما يستتبعه من ملاحظة وتطوير[1]. لذلك يمكن تعريفه بشكل عام بأنه علم استنباط نظم قادرة على حل المشاكل وأداء الوظائف بمحاكاة العمليات الذهنية، ويمكن تلقين الذكاء الاصطناعي كيفية دراسة وحل مشكلة ما بمفرده دون تدخل بشري، ويمكن للنظم المختلفة أن تبلغ مستويات مختلفة من التشغيل الذاتي وفي مقدورها أن تتصرف باستقلالية، ومن غير الممكن في هذا الخصوص التكهن بعمل تلك النظم ولا بنتائجها لأنها تتصرف باعتبارها صناديق سوداء.[2]

وتعلق بالذكاء الاصطناعي مصطلح "خوارزميات" Algorithm، وهي سلسلة محددة من العمليات أو التعليمات التي تسمح بحل فئة من المشاكل، مثل خوارزمية القسمة التي تحسب النسبة بين رقمين بدقة معينة، حيث يتم تصميمها لإنجاز مهام متنوعة للغاية، وبالتالي فإن استخراج قاعدة بيانات كبيرة من الأمثلة التي تحترم سلسلة من المعايير يتطلب خوارزمية، وفي هذه الحالة يهدف عملها إلى ضمان نتائج دقيقة ويتم استدعاؤها في وقت قصير حتى عندما تكون قاعدة البيانات كبيرة جدًا. وفي حالة الذكاء الاصطناعي تحدد كلمة "خوارزمية" الطريقة التي تجعل من الممكن تقديم استجابة لطلب ما عن طريق معادلة حسابية، وما يسمى بعملية "التعلم" التي جعلت من الممكن تحديد ذلك بدقة، معادلة هذه العملية الثانية هي التي تبرر تسمية "الذكاء الاصطناعي" لأنها تستند إلى تحليل عدد كبير من الأمثلة التي يفترض أن تستخرج منها "تلقائيًا" قواعد القرار لا سيما في سياق العمل القانوني[3] الذي نحن بصدد التعرض له في هذا البحث.

أهمية البحث وأهدافه:

بظهور تقنيات الذكاء الاصطناعي في مجال العدالة الجنائية أصبح من الضروري أن تضاف للمكتبة القانونية الأبحاث القانونية التي تحاول أن تتناول ماهية هذه التقنيات وأنواعها وصورها المختلفة ومجالات استخدامها لدى أجهزة العدالة الجنائية، والصعوبات التي قد تكتنف وظائفها، وبيان ما سمحت به الدراسة من التشريعات الإماراتية التي بدأت في تقنينها، أو توصيات الجماعة الدولية التي وضعت الضوابط اللازمة لنجاعة خدمات هذه التقنيات، وفي تقدير الباحث أن الأمر به الكثير

(1) آلان بونيه - الذكاء الاصطناعي واقعه ومستقبله – ترجمة د/علي صبري فرغلي – سلسلة عالم المعرفة – الكويت – عدد أبريل 1993 – صـ 11 وما بعدها.

(2) الجوانب القانونية للعقود الذكية والذكاء الاصطناعي – ورقة عمل مقدمة من تشيكيا إلى لجنة الأمم المتحدة للقانون التجاري الدولي – الدورة الحادية الخمسون – نيويورك 25 من يونيو – 13 يوليو 2018 – مطبوعات الجمعية العامة للأمم المتحدة – 960/A/CN.9 – صـ 2.

(3) Laurence Pécaut-Rivolier et Stéphane Robin, consulté le 08/01/2021, Justice et intelligence artificielle, préparer demain : regards croisés d'une juriste et d'un mathématicien | Dalloz Actualité (dalloz-actualite.fr).

من التفصيل الذي لا تتسع له هذه السطور، ولكن هذا لا يمنع من محاولة وضع لبنات أولية للبناء عليها من طلبة العلم، حتى الوصول إلى الإطار التقني والتشريعي الذي تستقيم به العلاقة بين آفاق التكنولوجيا وأخلاقيات وثوابت القانون.

إشكالية البحث:

لا يخفى على مُنصِف جدة موضوع البحث، ومن ثمّ قلة مصادره التشريعية والقضائية والفقهية ولا سيما العربية منها، وهو ما يطرح عدة تساؤلات حول كيفية توظيف تطبيقات الذكاء الاصطناعي في خدمة العدالة الجنائية، وهل من الممكن أن تجعل تحقيق العدالة الجنائية أقل كلفة، ودمج القضايا ذات الوقائع المتشابهة لمحاولة إصدار أحكام مسببة تسبيبًا واحدًا، وهل نتائج الخوارزميات مطروحة بصفة استشارية أم يبقى القرار الأخير لأفراد أجهزة إنفاذ القانون، وهل البيانات التي تم إدخالها في الخوارزمية مقدمة بشكل قانوني وستستخدم لغرض قانوني، وهل مقترحات الخوارزميات مفصلة بشكل كاف، وإلى من تعود ملكيتها والبيانات التي أدخلت فيها، وهل تمتلك أجهزة العدالة حقوق استخدامها، وهل سيتم صيانة النظام وتحديثه وتأمينه حسب الحاجة، وما هي آليات المراقبة والتحقق من نتائج الخوارزميات، وهل يمتلك المستخدمون الخبرة اللازمة للتعامل معها؟ وهو ما سيحاول البحث الإجابة عنه لمحاولة تنظيم مستقبل التشريعات القانونية المتعلقة بتقنيات الذكاء الاصطناعي.

منهج البحث:

اتبع الباحث المنهج الوصفي التحليلي لدراسة ظاهرة الذكاء الاصطناعي ودوره الداعم لأنظمة العدالة الجنائية من خلال تعريفه، وبيان وظائفه، ومدى تأثيره على أطراف منظومة العدالة الجنائية، وبيان مخاطره لدى القائلين بها، واستعراض وتحليل بعض نصوص التشريعات الإماراتية ذات الصلة بموضوع البحث، فضلًا عن التوصيات الدولية التي حرصت على وضع مبادئ لاستخدامات الذكاء الاصطناعي في أنظمة العدالة.

خطة البحث:

احتوت هذه الدراسة على مقدمة ومبحثين وخاتمة.
المبحث الأول: دور الذكاء الاصطناعي في جمع الأدلة الجنائية.
المبحث الثاني: دور الذكاء الاصطناعي في أنظمة المحاكمات الجنائية.

المبحث الأول
دور الذكاء الاصطناعي في جمع الأدلة الجنائية

يُعد نظام العدالة الجنائية أحد الاختصاصات الرئيسة للدولة لضمان عدم الإخلال بالنظام أو الآداب العامة ومنع انتهاكات الحقوق المختلفة للأفراد والمؤسسات، وكشف الجرائم الجنائية، والتحقيق فيها، وملاحقتها قضائيًا ومعاقبة الجناة، لذلك فهو ذلك النظام الذي يمنح سلطات هائلة للدولة في استخدام وسائل التحري عن الجرائم والقبض على مرتكبيها وتفتيش المشتبه بهم وحبس المتهمين احتياطيًا فضلًا عن الحكم بالسجن والإعدام والغرامة والمصادرة، ولغايات استخدامات أجهزة الشرطة لأدوات التطور العلمي في مجالات العدالة الجنائية فقد بدأت بعض الشركات تدشين تطبيقات الذكاء الاصطناعي التي من شأنها التعرف على الوجه، وتحديد الضحايا المحتملين للجريمة، وتقييم مخاطر الاحتجاز السابق على المحاكمة، والحكم والإفراج المشروط.

إن تطبيق القانون بشكلٍ عام هو نشاط قائم على المعلومات وجمعها ومعالجتها والتصرف بموجبها من أجل منع الجريمة أو السيطرة عليها، ولا شك في أن الذكاء الاصطناعي والروبوتات[1] هما مفهومان جديدان ساعدت بعض تطبيقاته المثيرة للاهتمام في إنفاذ القانون كأدوات افتراضية للمساعدة في تحديد سبب الوفاة، والتنبؤ بمكان ونوع الجرائم المحتمل حدوثها، وبرامج الرؤية الحاسوبية للتعرف على السيارات المسروقة أو المشتبه باستخدامها في الجرائم، وتلك التي تحدد الأطفال الخاضعين للاستغلال الجنسي، فضلًا عن أدوات تحديد المخادعين عبر الإنترنت ومعاقبتهم، وتتبع التدفقات المالية غير المشروعة، والطائرات بدون طيار لمراقبة السجون والحدود، وأدوات تحليل الأصوات والمقاطع المصورة لرصد السجناء الخطرين، وآلات تدوين الأقوال لدعم التحقيقات الجنائية، فضلًا عن الروبوتات المستقلة التي يمكنها فحص الأشياء

(1) عرفت المادة الأولى من المرسوم بقانون اتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية الصادر في 20 من سبتمبر 2021 والنافذ اعتبارًا من 02 من يناير 2022 الروبوت الإلكتروني وهو أحد استخدامات الذكاء الاصطناعي بأنه "برنامج إلكتروني يتم إنشاؤه أو تعديله لغرض تشغيل المهام المؤتمتة بكفاءة وسرعة".

المشبوهة والخطيرة مثل المتفجرات[1]. كل ما سلف يساعد أجهزة الشرطة في منع الجرائم وجمع الأدلة الجنائية، وهو ما نستطيع طرحه فيما يلي:

المطلب الأول

دور الذكاء الاصطناعي في منع الجرائم المحتملة

تقوم جهات الضبط القضائي على حفظ النظام العام ومراقبة تطبيق القوانين وتأمين الحماية للسكان وحفظ الجانب الأخلاقي العام، وهو ما يلقي على عاتقها وقاية المجتمع من الجرائم المحتملة الوقوع، ونفاذًا لذلك ساهمت تقنيات الذكاء الاصطناعي في مساعدة رجال الشرطة الجنائية على التنبؤ بالجريمة قبل وقوعها من خلال بعض التقنيات والاستخدامات التي يمكن استعراضها فيما يلي:

أولًا: تقنية بريدبول PredPol للتنبؤ بالجرائم:

تهدف **PredPol** إلى مساعدة أجهزة إنفاذ القانون في الحفاظ على المجتمعات أكثر أمانًا من خلال ما يسمى بالشرطة التنبؤية **Predictive Policing** التي تتمثل ممارستها في تحديد الأوقات والأماكن التي يُرجح فيها حدوث جرائم معينة، ثم تسيير دوريات في تلك المناطق لمنع حدوث تلك الجرائم. حيث تحدد أداة العمليات اليومية مكان وزمان حدوث الجريمة على الأرجح، مما يتيح للشرطة تخصيص مواردها بشكل فعال لمنع الجريمة. وتعتمد توقعاتها على استخدام ثلاثة عناصر بيانات فقط وهي: نوع الجريمة، مكان ارتكاب الجريمة، وتاريخ ووقت ارتكابها، باعتبارها بيانات الإدخال الأكثر دقة للتنبؤ. فيما تعلن **PredPol** أنه يتم استخدامها حاليًا للمساعدة في حماية شخص من بين كل 33 شخصًا في الولايات المتحدة. وقد نشأ بريدبول من مشروع بحثي من خلال العمل مع علماء الرياضيات وعلماء السلوك بين إدارة شرطة لوس أنجلوس وجامعة كاليفورنيا في لوس أنجلوس وجامعة سانتا كلارا، حيث قام الفريق بتقييم مجموعة متنوعة من

(1) Interpol & Unicri (United Nations Interregional Crime and Justice Research Institute), Artificial Intelligence and Robotics For Law Enforcement, Available on Line on 10/01/2021 at: https://www.europarl.europa.eu/cms-data/196207/UNICRI.

نظم الإنتربول بالتعاون مع معهد أبحاث الجريمة والعدالة التابع للأمم المتحدة (UNICRI) الاجتماع العالمي الأول لاستعراض فرص ومخاطر الذكاء الاصطناعي والروبوتات في إنفاذ القانون في سنغافورة في 11 و12 يوليو 2018، وناقش الحضور كيف يمكنهم استخدام التقنيات من قبل جهات إنفاذ القانون لدعم أنشطتها، وتقييم الإمكانات والتحديات التي يتعين معالجتها والتغلب عليها، حيث يلخص هذا التقرير التحديات والنتائج الرئيسية والتوصيات التي جرى مناقشتها خلال الاجتماع.

أنواع البيانات ونماذج السلوك والتنبؤ لإيجاد طريقة لاستخدام البيانات الشرطية ومحاولة فهم ما إذا كانت هذه البيانات يمكن أن تقدم أي توصيات استشرافية حول مكان وزمان حدوث جرائم إضافية قد تعطي القدرة على توقع مواقع وأوقات هذه الجرائم بما يسمح بنشر عناصر الشرطة بشكل استباقي للمساعدة في منع وقوع هذه الجرائم[1].

إلا أن البعض يشكك في نجاعة خوارزمية بريدبول ويخشى انتهاكها لحقوق الإنسان بإخفاء عنصرية بعض ممارسات الشرطة من خلال البيانات التي يتم ابتداءً إدراجها في النظام ذاته، لا سيما فيما يتعلق بمكان ارتكاب الجرائم، فعلى سبيل المثال إذا كانت قوات الشرطة في الماضي تركز بشكل غير متناسب على حي معين، لكان من المرجح أن يتم الكشف عن الجرائم المرتكبة في نفس الحي، ما سيؤدي بعد ذلك إلى تشويه تاريخ البيانات المستخدمة لإنشاء خوارزمية **PredPol** بشكل مصطنع، حيث ستتنبأ باحتمالية أعلى لارتكاب الجرائم في هذا الحي مستقبلًا، وهو ما سيؤدي بالضرورة إلى تخصيص الشرطة للمزيد من الموارد لحفظ النظام في هذا الحي، فإذا كان من يسكنه في الغالب أشخاص من عرق أو دين معين، والذي قد يكون السبب الحقيقي للاهتمام الخاص الذي أولته الشرطة في البداية هو هذا "التنميط العرقي"، فإن نتائج الخوارزمية قد تكون تمييزية لأسباب يحظرها القانون الدولي لحقوق الإنسان[2].

ثانيًا: تقنية HART للمساعدة في تقييم المخاطر:

إذا ما تخيلنا أنه تم القبض على حائز مخدرات ليس لديه سوابق جنائية عن أي جرائم عنيفة أو خطيرة، فما هو القرار الأنجع هل الإفراج عنه بكفالة أم حبسه احتياطيًا؟ حيث أن الأخير قد يهدر الموارد والأموال، وقد يضر أكثر مما ينفع، لذلك فإن هذا السؤال يطرح نفسه ملايين المرات سنويًا في جميع أنحاء العالم، والإجابة عنه تعتمد على مدى احتمال أن يتسبب المتهم في ضرر كبير إذا ما تم إطلاق سراحه.

لذلك في منتصف عام 2016 قام الباحثون بجامعة كامبريدج بالتعاون مع شرطة دورهام بالمملكة المتحدة بتثبيت أول أداة لمساعدة الشرطة في اتخاذ قرارات الاحتجاز في **Durham Constabulary** استخدمت فيها تكنولوجيا الذكاء الاصطناعي المسماة أداة تقييم المخاطر

(1)PredPol is The Market Leader in Predictive Policing - Available online on 29/12/2020 at: https://www.predpol.com/about/

(2) Council of EUROPE - Parliamentary Assembly - Justice par algorithme – le rôle de l'intelligence artificielle dans les systèmes de police et de justice pénale, consulté le 15/12/2020 https://pace.coe.int/fr/files/25062#trace-1, Sections 26 and 27.

(HART) بالنظر إلى التاريخ الإجرامي على مدار خمس سنوات لعدد 104,000 من الأشخاص الذين تم اعتقالهم في شرطة دورهام، بالإضافة إلى العمر والجنس والمنطقة الجغرافية، وكان الهدف من HART هو تصنيف ما إذا كان المتهم معرضًا في العامين المقبلين لارتكاب جريمة خطيرة جديدة مثل القتل أو الجرائم الجنسية أو السطو؛ أم أنه معتدل الخطر ومرشح لارتكاب (جريمة غير خطيرة) ؛ أو منخفض المخاطر (من غير المرجح أن يرتكب أي جريمة). وبواسطة تقنية HART أرادت شرطة دورهام تحديد مجموعة المشتبه بهم ذوي "المخاطر المعتدلة" حتى يمكنهم الاستفادة من برنامج نقطة التفتيش Checkpoint، والذي يهدف إلى معالجة الأسباب الجذرية للجريمة وتقديم بديل عن محاكمتهم جنائيًا لغايات تحويلهم إلى فئة "المخاطر المنخفضة". وقد وجدت دراسة التحقق المستقلة لـ HART دقة إجمالية بلغت حوالي 63%، ومما لا شك فيه فإن الذكاء الاصطناعي قابل للتعديل بشكل لا نهائي، كما أن مخرجات تقنية HART إرشادية فقط، وأن القرار النهائي يرجع للضابط المسؤول في نطاق سلطة شرطة دورهام، فالتقنية تدعم صانع القرار البشري ولا تستبدله[1].

ثالثًا: تقنية كومباس COMPAS لتقييم خطر العودة إلى الإجرام:

يُستخدم نظام كومباس من قبل عدة ولايات في الولايات المتحدة لتقييم خطر عودة الفرد إلى الإجرام، باعتباره أداة تقييم مخاطر باستخدام ثلاثة مقاييس وهي "خطر الإفراج قبل المحاكمة" أي خطر عدم الظهور وإعادة الاعتقال لارتكاب جريمة؛ و"العود العام" أي ارتكاب جريمة جديدة في غضون عامين؛ و"العود العنيف" أي ارتكاب جرائم عنيفة، وقد بدأ قضاة ولاية نيويورك استخدامه لاختيار العقوبة المفروضة، وفي فلوريدا تم استخدامه لتقرير ما إذا كان يجب حبس المتهم أو الإفراج عنه بكفالة، وفي ولاية ويسكونسن تم استخدامه في مراحل نظام السجون من صدور الحكم حتى الإفراج المشروط[2].

وتم اختبار هذه التقنية بتحقيق أجرته شركة ProPublica عام 2016 فوجدت أنه من المرجح تحديد المتهمين السود كمجرمين في المستقبل، وتصنيفهم على هذا النحو بما يعادل ضعف معدل المتهمين البيض، لكن المحققين وجدوا أيضًا أن فقط 20% من الأشخاص الذين توقعوا لهم

(1) Cambridge University – Helping police make custody decisions using artificial intelligence –Available online on 29/12/2020 at: https://www.cam.ac.uk/research/features/helping-police-make-custody-decisions-using-artificial-intelligence.

(2)Council of EUROPE - Parliamentary Assembly - Justice par algorithme – le rôle de l'intelligence artificielle dans les systèmes de police et de justice pénale, Référence précédente, - Sections 26 and 27.

ارتكاب جرائم عنيفة فعلوا ذلك عند النظر في مجموعة كاملة من الجرائم بما في ذلك الجنح، وبينما تم القبض على 61% من المشتبه بعودتهم للإجرام بسبب أي جرائم لاحقة في غضون عامين تبين أنه نشأت بعض الحسابات الخاطئة للمخاطر من المدخلات غير الدقيقة وعلى سبيل المثال الفشل في الحصول على السجل الجنائي لسابقة سجن شخص ما من ولاية أخرى، في حين تُعزى النتائج الأخرى إلى طريقة تقييم العوامل وعلى سبيل المثال فقد يكون الشخص الذي تحرش بطفل يتم تصنيفه على أنه منخفض المخاطر فقط لأن لديه وظيفة [1].

وبالرغم من أن أدوات تقييم المخاطر باستخدام خوارزميات الذكاء الاصطناعي قد يكون لها بعض العيوب بسبب اعتمادها على بيانات الاعتقال أو الاحتجاز السابق كنقطة البداية لتحليل التنبؤ بجريمة مستقبلية ما لم تعتمد تلك التنبؤات إلى حدٍ كبير على جودة البيانات المدرجة في تلك الأداة؛ ومع ذلك فإن العديد من هذه الأدوات المتاحة لا تكشف عن خوارزمياتها أو منهجيات وطرق عملها، مما يجعل من الصعب على المحامين تحدي نتائجها.

كما يمكن لتنامي استخدام الأدوات الاصطناعية في إنفاذ القانون أن يُنشئ مخاوف بشأن حقوق المواطنين الأساسية، وقدرات البحث والمصادَرة المتزايدة المتوفرة لمؤسسات إنفاذ القانون وما يرافقها من تآكل للخصوصية هي أكثر ما يثير المخاوف، أو استخدام الروبوتات في القبض على المخالفين للقانون، إذ انتهى حدث إطلاق نار جماعي مؤخرًا في الولايات المتحدة بمقتل مُطلِق النار بقنبلةٍ أطلقها عليه روبوت Murphy,2016، فأعرب بعض المراقبين عن انزعاجهم من هذا التطور الجديد الذي طرأ على إنفاذ القانون، وما قد يعنيه من حيث قرينة البراءة، والسؤال الذي يطرح نفسه هو هل من المحتمل أن تُسهم الأخطاء غير المتوقعة للأتمتة[2] في تقويض جهود الثقة بين المواطنين والدولة على نحوٍ لا داعي له؟ فضلًا عن ذلك فقد بدأ علماء القانون يستكشفون آثارًا أخرى مرتبطة بالشخصية القانونية التي ربما تتمتع بها الأدوات الاصطناعية من خلال النظام الأساسي للشركات، فربّما يشكّل ذلك مجالًا قانونيًا حديثًا[3].

(1)Algorithms in the Criminal Justice System: Risk Assessment Tools - Available online on 29/12/2020 at: https://epic.org/algorithmic-transparency/crim-justice/

(2) عرفت المادة الأولى من المرسوم بقانون اتحادي إماراتي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية الصادر بتاريخ 20 سبتمبر 2021 والمعمول به اعتبارًا من 2 يناير 2022 المعالجة المؤتمتة بأنها "المعالجة التي تتم باستخدام برنامج أو نظام إلكتروني يعمل بطريقة آلية وتلقائية إما بشكل مستقل كليًا دون أي تدخل بشري أو بشكل جزئي بإشراف وتدخل بشري محدود".

(3) Osonde A. Osoba & William Welser IV - Previous reference, P.8.

رابعًا: دور الكاميرات المحمولة على الجسم في منع الجرائم كإحدى تطبيقات العدالة الجنائية الذكية:

صدر قرار حاكم دبي رقم 14 لسنة 2020 بشأن استخدام الكاميرات الأمنية في توثيق مهام منتسبي الشرطة [1] وهم الضابط وصف الضابط والفرد من العاملين في الشرطة ويشمل الذكر والأنثى، بينما الكاميرا الأمنية هي كل جهاز مُعدّ لالتقاط ونقل وتسجيل الصوت والصورة يستخدمه المنتسب أو الشرطة، ويهدف هذا القرار إلى رفع مستوى جودة الخدمات المقدمة من الشرطة، وتطوير أداء المنتسبين وبث روح الطمأنينة لدى أفراد المجتمع، وترسيخ شعورهم بالأمن والأمان والمحافظة على حقوق أفراد المجتمع عند تعاملهم مع المنتسبين، والوقوف على سلوك المنتسبين عند تعاملهم مع أفراد المجتمع، لقياس مستوى الشفافية والحيادية لديهم، والتحقق من الممارسات المنسوبة إليهم، فضلًا عن المساهمة في إثبات الجرائم، ويكون لمحتوى تسجيلات الكاميرات الحجية على الكافة، ما لم يثبت لسلطة البحث والتحري بالشرطة أو للسلطة القضائية المختصة خلاف ذلك.

ويشير بعض الفقه إلى أن الكاميرات المحمولة على الجسم تشكل إحدى الطرق المتاحة لمواجهة التحديات المرتبطة بالعمل الشرطي وتحسن ممارسات إنفاذ القانون بشكل عام، إذ من شأنها عرض المعلومات في الوقت الفعلي عند استخدامها، وتزويد موظفي إنفاذ القانون بأداة مراقبة لتعزيز سلامة رجال الشرطة وكفاءتهم ومنع الجريمة، وتضيف شفافية أفضل بزيادة درجة التحضر في تصرفات المواطنين ورجال الشرطة، وسرعة اتخاذ القرارات بشأن شكاوى المواطنين، وزيادة قوة الأدلة الجنائية، وتحديد الاحتياجات التدريبية بشكل علمي ودقيق.

وفي تفصيل ذلك يمكن للكاميرات المحمولة أن تؤدي إلى تحسين شرعية سلطات إنفاذ القانون، إذ تعاني العديد من المجتمعات من مشكلة غياب الثقة في سلطات إنفاذ القانون، وتتفاقم هذه المشكلة عند طرح الأسئلة المتعلقة بتواصل رجال الشرطة مع أفراد المجتمع، والتي غالبًا ما تنطوي على استخدام القوة، ولمواجهة هذه المشكلة فإن مشاهد الفيديو التي يتم التقاطها خلال هذه اللقاءات قد توفر توثيقًا أفضل للحوار الذي تم بين رجل الشرطة والفرد، مما يساعد في تأكيد طبيعة الأحداث وتأييد الروايات التي يقدمها رجل الشرطة وأفراد المجتمع، فضلًا عن ارتفاع معدل امتثال المواطنين لأوامر رجال الشرطة خلال اللقاءات التي تجمع بينهم، الأمر الذي يقود بالتالي إلى انخفاض عدد الشكاوى المرفوعة ضد سلطات إنفاذ القانون، وفي كثير من الأحيان

(1) قرار حاكم دبي رقم 14 لسنة 2020 بشأن استخدام الكاميرات الأمنية في توثيق مهام منتسبي الشرطة – صدر في 13 من أغسطس 2020 ونشر في الجريدة الرسمية لحكومة دبي السنة 54 العدد 483 بتاريخ 19 أغسطس 2020م.

يغير المواطنون سلوكهم تجاه رجال الشرطة عند إبلاغهم بتسجيل اللقاء بما يمنع من تصعيد بعض المواقف إلى مستويات تتطلب استخدام القوة.

كما تؤدي الكاميرات المحمولة إلى اتخاذ قرارات أسرع بشأن شكاوى ودعاوى المواطنين التي تدعي الاستخدام المفرط للقوة وأشكال أخرى لسوء سلوك رجال الشرطة. وفي تحقيقات القضايا التي تتضمن روايات غير متسقة للقاء الحاصل ما بين الطرفين، حيث غالبًا ما تفتقر هذه التحقيقات إلى أدلة مؤيدة، ويتم إغلاقها لاحقًا عند عدم وجود مقطع فيديو أو شهود عيان مستقلين أو متعاونين، ومن شأن ذلك أن يقلل من الثقة في تطبيق القانون، ويخلق مزاعم بأن سوء المعاملة لم يتم التعامل معها بالشكل الملائم، ومن هنا تأتي أهمية الفيديوهات التي تلتقطها الكاميرات المحمولة، حيث تساعد في تأكيد وقائع اللقاء بين رجل الشرطة والشاكي، مما يؤدي إلى اتخاذ قرار أسرع. كما أنها دليل في حالات القبض أو الملاحقات القضائية مع تقليل إجمالي الوقت المطلوب من مأموري الضبط القضائي لاستكمال الأعمال الورقية في ملفات القضايا وتأكيد الأدلة المقدمة من النيابة، وارتفاع عدد الإقرارات بالذنب في إجراءات المحاكمة[1] .

خامسًا: دور الذكاء الاصطناعي في مواجهة الاحتيال المصرفي:

ثمة مثال ناجح لتطبيقات الذكاء الاصطناعي من الناحية المصرفية يعرف باسم "Authorizes Assistant" تم تصميمه لشركة أمريكان اكسبريس لمساعدة العناصر البشرية المخول إليها منح القروض، فقد كان هذا النظام يعطي التوجيهات معتمدًا على مجموعة من البيانات عن العميل طالب القرض تتضمن معلومات حول حسابه الخاص، وأساليب إنفاقه، وبياناته الشخصية، ومن خلال دراسة العديد من قواعد البيانات يقوم النظام بتقديم "توصية" بشأن اعتماد منح القروض للعملاء، ويمكن لهذا النظام أن يمد الشخص المفوض باعتماد منح القرض بأية حقائق أخرى ينبغي وضعها في الاعتبار فيما يتعلق بهذا العميل[2] . لذلك كان استخدام هذا النظام وغيره من الأنظمة القائمة على المعرفة لمساعدة البشر في اتخاذ القرارات السريعة بالاعتماد على البيانات التي يمكن تخزينها في عدد من قواعد البيانات الإلكترونية يجسد نظم مواجهة محاولات الاحتيال على المصارف للشروع في الحصول على قروض لا تستند إلى معلومات صادقة، أو بيانات واضحة، أو ضمانات كافية.

(1) الأستاذ الدكتور/ أحمد عبد الظاهر – العدالة الجنائية الذكية – الكاميرات المحمولة على الجسم - دراسة منشورة بمجلة القضاء والقانون – دائرة القضاء – السنة السابعة العدد 8 - أكتوبر 2020 – صـ 60 وما بعدها.

(2) الذكاء الاصطناعي – بلاي ويتباي – ترجمة دار الفاروق للاستثمارات الثقافية باتفاقية نشر مع مؤسسة محمد بن راشد آل مكتوم – طبعة 2008 - صـ 61 وما بعدها.

المطلب الثاني

دور الذكاء الاصطناعي في كشف الجرائم المرتكبة

لا تقتصر مهام مأموري الضبط القضائي على منع الجرائم فحسب، بل عليهم أيضًا تقصي الجرائم التي وقعت والبحث عن مرتكبيها وجمع المعلومات والأدلة اللازمة للتحقيق والاتهام، واتخاذ جميع الوسائل التحفظية اللازمة للمحافظة على أدلة الجريمة[1]، وقامت تقنيات الذكاء الاصطناعي بتعزيز جهود الشرطة في هذه المهام على النحو التالي:

أولًا: دور الذكاء الاصطناعي في التعرف على صور المجني عليهم والمشتبه بهم:

حينما يكون من واجبات أفراد الشرطة البحث عن المجني عليهم أو الجناة والمشتبه بهم أو الفارّين من العدالة، فذلك يتطلب التعرف على العشرات والمئات بل والآلاف من صور الوجه للمساعدة في تحديد هوية الفرد ومكان وجوده، إلا أن عملية فحص العدد الهائل من الصور أو مقاطع الفيديو ذات الصلة بالأشخاص المطلوبين بشكل دقيق وفي الوقت المناسب هي مهمة شاقة وتستغرق وقتًا طويلًا، وتتطلب أعدادًا هائلةً من ذوي الخبرة في هذه المهام، فضلًا عن احتمال حدوث خطأ بشري بسبب الإرهاق وغيره من العوامل، إلا أن تقنيات الذكاء الاصطناعي وفرت قدرة التغلب على هذه المصاعب، فباستخدام الخوارزميات أمكن التمييز بين ملامح وجه شخص وآخر مثل شكل العيون ولونها والمسافة بينها للتعرف عليها، ومطابقة الوجوه وغيرها من الأشياء التي تساعد على اكتشاف الجرائم أو مرتكبيها بعد وقوعها استجابة لاحتياجات العدالة الجنائية وإنفاذ القانون.

ولذلك قام باحثون في جامعة تكساس في دالاس بالشراكة مع مكتب التحقيقات الفيدرالي والمعهد الوطني للمعايير والتكنولوجيا بتطوير خوارزمية في عام 2017 تستطيع في 30 ثانية فحص وتقييم الوجوه والتعرف على البشر، بل واستجابة للحاجة إلى جودة أعلى للمعلومات وبشكل أكثر فاعلية تقوم جامعة كارنيجي ميلون على تطوير خوارزميات الذكاء الاصطناعي لتحسين الاكتشاف والتعرف على الصور التي يتم فيها التقاط وجه الفرد من زوايا مختلفة أو جزء من جانب الوجه عندما ينظر الفرد بعيدًا عن الكاميرا أو تحجبه الأقنعة أو المصابيح أو الإضاءة، وتكوين صورة للوجه حتى إذا كانت منخفضة الجودة أو ذات دقة ضعيفة وكانت الإضاءة المحيطة بها منخفضة، حيث تجعل

(1) راجع نص المادتين 30 و35 من قانون الإجراءات الجزائية الاتحادي الإماراتي.

الخوارزمية جودة الصورة مطابقة للوجه والتي يمكن لها المساعدة في تحديد المشتبه بهم أو المساعدة في التحقيقات الجنائية.

كما يجري عبر تقنيات الذكاء الاصطناعي استكشاف فكرة "فهم المشهد" Understanding Scene، أو القدرة على تطوير وصف وإيجاد العلاقة بين (الأشخاص، والأماكن، والأشياء) في سلسلة من الصور ومقاطع الفيديو لتقديمها في سياق متصل لفك رموز الجريمة، فعلى سبيل المثال، قد تكون صورًا تم التقاطها لشخص ما قام بسحب مسدس من نافذة أحد المتاجر، فالهدف هنا هو اكتشاف الأنشطة التي من شأنها أن تساعد في تحديد الجرائم قيد الوقوع لمراقبة مرتكبيها والتدخل لمنعها في الوقت المناسب عبر مشاهد متعددة يمكن أن تشير إلى أهمية محتملة لبعض الأحداث التي يجب على جهات إنفاذ القانون الاطلاع عليها لتأكيدها ومتابعتها[1].

وكان تتبع الأطفال المفقودين والمخطوفين هو أكبر استخدام لتقنيات الذكاء الاصطناعي في التعرف على الوجوه، حيث بدأت الشرطة في الهند استخدامها في أماكن مختلفة مثل محطات السكك الحديدية والحافلات والأسواق المزدحمة وغيرها من الأماكن، حيث أثبتت الدراسات الإبلاغ عن اختفاء 63،407 طفل في العام 2016، و63،349 طفل في العام 2017، و67،134 طفل في العام 2018، وتشير البيانات إلى أن أسباب ذلك هو استخدامهم في التسول أو احتجازهم للحصول على فدية، وقد يتم تهريبهم إلى دول مختلفة وإجبارهم على ممارسة الدعارة أو حتى الانتقام، لذلك عمل نظام التعرف على الوجه الآلي (AFRS) على قراءة هندسة الوجه كالمسافة بين العينين والمسافة من الجبهة إلى الذقن، حيث يحدد البرنامج معالم الوجه، ويحدد نظام واحد 68 منها مفتاحًا لتمييز وتوقع الوجه[2]، وهكذا استحدثت تقنيات الذكاء الاصطناعي تعزيز جهود جهات إنفاذ القانون في سعيها لمكافحة أشكال العنف والاستغلال ومكافحة الجريمة والاعتداء الجنسي على الأطفال.

ثانيًا: دور الذكاء الاصطناعي في الطب الشرعي وتحليل الحمض النووي DNA:

يمكن للذكاء الاصطناعي أيضًا أن يفيد مجتمع إنفاذ القانون من وجهة نظر علمية لمعالجة الأدلة وذلك في اختبار الحمض النووي الذي كان له تأثير غير مسبوق في التعرف على المجرمين من

(1) Christopher Rigano, "Using Artificial Intelligence to Address Criminal Justice Needs" NIJ Journal 280, January 2019, https:// www.nij.gov/journals/280/Pages. – p.2 - 3

(2) Facial recognition tech can help trace missing children despite privacy handicap – Available on line 12/01/2021 at: https://www.indialegallive.com/column-news/artificial-intelligence-face-recognition-raise-niti-aayog/

خلال المواد البيولوجية، مثل الدم واللعاب والمني وخلايا الجلد، عن طريق التلامس مع الأشخاص والأشياء أثناء تنفيذ الجريمة. ومع تقدم تقنية الحمض النووي تقدمت حساسية تحليل الحمض النووي، مما يسمح لعلماء الطب الشرعي إعادة اكتشاف أو تفسير ومعالجة المستوى المنخفض أو المتدهور من أدلة DNA السابقة التي كانت غير قابلة للاستخدام من قبل، فعلى سبيل المثال الحمض النووي الذي تم الحصول عليه منذ عقود كدليلٍ في جرائم عنف كالاعتداءات الجنسية أو جرائم القتل التي لا يمكن اكتشاف الجناة فيها لصغر كميته أو لانخفاض جودته يتم الآن إعادة فتح تلك القضايا وتقديم هذه الأدلة إلى المعامل لإعادة التحليل في مختبرات الجريمة، مما يؤدي إلى إمكانية اكتشاف خليط الحمض النووي وفصله من عدة جناة قد ساهموا في الجريمة أو من شخص غير مرتبط بالجريمة على الإطلاق، وذلك باستخدام طرق حساسة للغاية بشأن عناصر الأدلة، ما يؤدي للمساعدة في تحقيق إنفاذ القانون.

ربما يكون للذكاء الاصطناعي القدرة على مواجهة هذا التحدي، حيث ينتج تحليل الحمض النووي كميات كبيرة من البيانات المعقدة في شكل إلكتروني؛ وتحتوي هذه البيانات على أنماط بعضها قد يكون خارج نطاق قدرة الإنسان على التحليل، ولذلك شارك باحثون في جامعة Syracuse University بالمشاركة مع مركز مقاطعة Onondaga لعلوم الطب الشرعي Forensic Sciences ومكتب مدينة نيويورك للفحص الطبي في علم الطب الشرعي Department of Forensic Biology للتحقيق في طريقة جديدة تقوم على التعلم الآلي لتفكيك خليط الحمض النووي وتحديد ملامحه الفردية لتقليل نقاط الضعف المحتملة، وتظهر الأبحاث أن تقنية الذكاء الاصطناعي لديها القدرة على المساعدة في ذلك[1].

كما طورت الشرطة في هولندا نظامًا للتعلم الآلي قائمًا على خوارزميات الذكاء الاصطناعي لمساعدتهم على تحديد القضايا القديمة والخطيرة والتي لم يتم الوصول إلى الجناة فيها، اعتمادًا على تقنية جديدة لم تكن موجودة في وقت التحقيقات الأولى وهي "رقمنة الملفات" بإدخالها في نظام الذكاء الاصطناعي الذي يحدد أولئك الذين لديهم أدلة واعدة يمكن إعادة فحصها في ضوء تقنيات الطب الشرعي الجديدة، ويأمل المسؤولون التوسع في هذا المشروع لتحديد القضايا التي يمكن حلها باستخدام بيانات غير جنائية، كالعلوم الاجتماعية ووسائل التواصل الاجتماعي وشهادة الشهود[2].

(1) Christopher Rigano, "Using Artificial Intelligence to Address Criminal Justice Needs, Previous reference, p- 6.

(2)Council of EUROPE - Parliamentary Assembly - Justice par algorithme – le rôle de l'intelligence artificielle dans les systèmes de police et de justice pénale, Référence précédente, Section 38.

ثالثًا: كشف الطلقات النارية Gunshot detection :

اكتشاف وتحليل أنماط الطلقات النارية التي استخدمت في الجريمة يقدم مجالًا آخر لاستخدام خوارزميات الذكاء الاصطناعي، ففي أحد مشاريع Cadre Research Labs, LLC قامت بتحليل الملفات الصوتية للطلقات النارية من الهواتف والأجهزة الذكية بحيث يمكن التوصل إلى نوعيتها باستخدام نموذج رياضي محدد جيدًا، والعمل على التفرقة بين أنواع الطلقات الصادرة من فوهة السلاح الناري المستخدم، وتحديد توقيت إطلاق النار، وعدد الأسلحة النارية الموجودة، وعدد الطلقات، كل ذلك يمكن أن يساعد سلطات إنفاذ القانون في التحقيقات[1].

وفي النهاية، لا ينال من أمان وتنظيم التكنولوجيا لحدٍ كبير طرح عدة مخاوف أخصها أن ملكية الشركات الخاصة لهكذا أنظمة الذكاء الاصطناعي والبيانات التي يعالجها النظام يمنحها إمكانية الاحتجاج بحقوق الملكية الفكرية الخاصة بها لرفض وصول مؤسسات الشرطة إلى مصدر التعليمات البرمجية، كما وقد لا يمتلك المستخدمون من أفراد الشرطة المعلومات أو التفسيرات اللازمة للحصول على كيفية عمل أو فهم بعض عمليات تطبيقات الذكاء الاصطناعي، فضلًا عن أن القوة التي قد يتمتع بها الذكاء الاصطناعي قد تكون مصحوبة بعدة مخاطر كسرعته، وتعقيده، وقابليته للتفوق على الذكاء البشري للمستخدم في مهام معينة، حتى ولاعتبارات الأمان في هذه التطبيقات وعدم قابليتها للاختراق فقد يكون من الصعوبة بمكان في بعض الأحيان معرفة الوسيلة أو الطريقة أو المنهجية المستخدمة لاستخراج نتيجة معينة من هذه التطبيقات.

كما أن استخدامات الذكاء الاصطناعي هي سلاح ذو حدين فقد يُمكّن الجماعات الإجرامية والإرهابية من الهجمات الإلكترونية، والاعتداءات الجسدية عن طريق الطائرات المُسيرة بدون طيار، ونشر الأخبار الكاذبة، فضلًا عن أدوات تغيير الوجوه والتزوير والتلاعب بالفيديو وتعريض الثقة في الشخصيات السياسية للخطر أو التشكيك في صحة الأدلة المقدمة في المحكمة. ليتضح أن مستقبل الذكاء الاصطناعي والروبوتات مليء بالتحديات، لذلك من المهم فهم مخاطر هذه التقنيات والاستعداد لها في مجال العدالة الجنائية للمساهمة في تعزيز قدرات إنفاذ القانون[2] .

(1) Christopher Rigano, "Using Artificial Intelligence to Address Criminal Justice Needs, Previous reference, P -7.

(2) Interpol & Unicri , Artificial Intelligence and Robotics For Law Enforcement, Previous reference.

المبحث الثاني

دور الذكاء الاصطناعي في أنظمة المحاكمات الجنائية

منذ يونيو 2019 دخل الذكاء الاصطناعي إلى المحاكم الصينية المسؤولة عن فحص جميع النزاعات المتعلقة بالإنترنت "محاكم الإنترنت"، ويتكون هذا البرنامج المسمى بـــ"قاضي الذكاء الاصطناعي" من قاضٍ افتراضي يظهر على الشاشة كإمرأة، يمتلك نفس تعابير الوجه، ويتحدث أيضًا بصوت أنثوي، واستنادًا إلى تقنيات تركيب اللغة والصورة الذكية تتمثل مهمة هذا القاضي الرقمي في مساعدة القضاة على إجراء عمليات متكررة، مثل تلقي المكالمات وتسهيل الإجراءات القانونية العادية، وهذا لا يمكن فهمه على أنه مجرد تحسين للكفاءة، إنه أيضًا تحسين للعدالة، حيث يسمح هذا النموذج بالفصل في القضايا بشكل أسرع، وفي المستقبل يجب على قضاة الذكاء الاصطناعي تقديم المساعدة لقضاة حقيقيين، والمساهمة في الأحكام من خلال جمع البيانات، كما سيقدم للمستخدمين نصائح في الوقت الفعلي لمساعدتهم على استخدام منصة التقاضي عبر الإنترنت[1].

وتعتبر الصين أول دولة تزود نفسها بالمحاكم الإلكترونية التي تسمح بمعالجة الملايين من قضايا المحاكم بواسطة قضاة آليين دون الحاجة إلى حضور المواطنين في المحكمة مع إجراء جلسة استماع للمحكمة الرقمية. وبين مارس وأكتوبر 2019 تم تسجيل أكثر من 3.1 مليون نشاط قانوني في هذه المحاكم [2]، إلا أنه إذا بدت الفوائد المستمدة من هذه الابتكارات التكنولوجية مهمة لإقامة العدالة، فإنها تبدو مع ذلك وكأنها تضعف "الكفاءة الرمزية" المتأصلة في ذاتية المحاكمة كضامن للعدالة الفعالة التي يجب ألا تتحقق فحسب، بل يجب أن يُنظر إليها على أنها تتحقق، فمن خلال العلاقة والشعور بالمكان والزمان فإن الثورة الرقمية من خلال الذكاء الاصطناعي تهدد الفعالية الرمزية للمحاكمة الجنائية. حيث تعتبر طقوس المحاكمة مرحلة مهمة لأطراف الدعوى الجنائية، لأنها تتيح تغيير عقيدة المحكمة من خلال قوة مرافعات دفاع الادعاء العام والمتهمين، والنقاشات الشفوية للمجني عليهم وشهود الإثبات والنفي، والتي تساهم غالبًا في ظهور أدلة

(1) Les "juges virtuels" font leur apparition dans les tribunaux chinois - consulté le 05/01/2021 https://www.rtbf.be/info/monde/detail_la-technologie-de-l-intelligence-artificielle-fait-son-apparition-dans-les-tribunaux-chinois?id=10383210

(2) Camille Guillard - La justice prédictive et l'IA dans le procès pénal : risques et opportunités - consulté le 15/12/2020 https://www.justicepenale.net/post/la-justice-prédictive-et-l-ia-dans-le-procès-pénal-risques-et-opportunités.

جديدة من خلال الاعترافات اللازمة لكشف الحقيقة القضائية التي تؤدي إلى اليقين القانوني بالبراءة أو الإدانة.

بيد أن إدخال الذكاء الاصطناعي في أنظمة المحاكمات الجنائية أصبح مرتبطًا بالعديد من القطاعات ذات الصلة التي تأمل في حدوث تطورات مختلفة جدًا في الواقع، فهناك من يتولى قضاء الحكم، ومن يتولى الادعاء العام، وأمناء السر، والمُحضرين، وموظفي المحاكم بشكلٍ عام فضلًا عن المحامين والخبراء والمترجمين، وهناك من يستخدم العدالة أو يعتمد عليها، والتي تسمى في المصطلحات القانونية "المتقاضين" من المجني عليهم أو المتهمين والشهود، كما وهناك وزارة العدل التي تصمم وتستخدم أدوات العدالة [1].

ولا جدال في تراكم العديد من القضايا في المحاكم خلفتها المنازعات بين البشر، وحيث يحفز القانون إلهام الفقيه الذي يجب عليه دومًا التعامل مع فكرٍ محوسب، ولذلك باتت مسألة الذكاء الاصطناعي في المحاكمات الجنائية تثير الإعجاب والخوف في ذات الوقت بين القانونيين والمتقاضين، إلا أنه من خلال تحليل البيانات القضائية، فإن ما يسمى بـ "العدالة التنبؤية" Prédictive Justice [2] أي ادعاء القدرة على "التنبؤ" بالنتائج المستقبلية قد تساهم في زيادة اليقين القانوني، عبر تسهيل الوصول إلى المعلومات القانونية والسوابق القضائية. بل وتسعى حتى للتنبؤ بالقرارات القضائية من خلال التحليل الاستقرائي، إلا أن البعض يصم هذا المصطلح بالخاطئ لأن التنبؤ ليس غاية في حد ذاته، كما أن الوعد بالتنبؤ لا يعتمد على أي يقين، لذلك فضلوا تعبير "العدالة التحليلية" Justice Analytique [3] اعتمادًا على الغرض من الذكاء الاصطناعي وهو تحليل قرارات العدالة التي اتخذت في الماضي لتحديد احتمالية النجاح في القضية اللاحقة، ولما كان الحاضر يشهد آفاق المستقبل في استخدامات الذكاء الاصطناعي في أنظمة العدالة الجنائية، وقد تعتبر علاجًا لبطء العدالة المستشري في العديد من الدول، ويمكنها أن تقلل تكاليفها وتوفر وسيلة لجعلها أكثر يقينًا، ومن هنا لا يمكن إهمال تقنيات "رقمنة" القطاع القانوني كقيمة أساسية

(1)Laurence Pécaut-Rivolier et Stéphane Robin, Référence précédente.

(2) Charte éthique européenne d'utilisation de l'intelligence artificielle dans les systèmes judiciaires (coe.int) - COMMISSION EUROPEENNE POUR L'EFFICACITE DE LA JUSTICE (CEPEJ) - Adoptée lors de la 31e réunion plénière de la CEPEJ (Strasbourg, 3-4 décembre 2018 - Conseil de l'Europe – consulté le 30/12/2020, P.14. الميثاق الأوروبي الأخلاقي لاستخدام الذكاء الاصطناعي في أنظمة العدالة وبيئتها – الصادر عن المفوضية الأوروبية لكفاءة العدالة (CEPEJ) اعتمد في الجلسة العامة رقم 31 بمدينة ستراسبورغ 3 – 4 ديسمبر 2018 - مجلس أوروبا.

(3) Camille Guillard, La justice prédictive et l'IA dans le procès pénal : risques et opportunités, Référence précédente,Où elle a indiqué l'expression qu'il a utilisée par Louis Larret-Chahine, co-fondateur de la legaltech française Predictice.

لإصلاح العدالة، وهو ما نحاول تسليط الضوء عليه فيما يلي:

المطلب الأول

دور الذكاء الاصطناعي في دعم اتخاذ القرار القضائي

يجب التسليم ابتداءً بأن توافر البيانات هو شرط أساسي لتطوير الذكاء الاصطناعي، مما يسمح له بأداء مهام معينة كان يقوم بها البشر في السابق بطريقة غير آلية، وكلما توفرت المزيد من البيانات زادت قدرة الذكاء الاصطناعي على تحسين نماذج التنبؤ. لذلك يمكن النظر بعين الاعتبار لتشريعات سمحت باستخدام المعلومات الواردة في الوثائق الإدارية الصادرة من قبل أي من إدارات الدولة لغرض إنجاز مهام خدماتها العامة، فمثلًا واعتبارًا من الأول من يناير للعام 2017 أصدرت فرنسا قانون "الجمهورية الرقمية" لتبادل المعلومات العامة بين إدارات الدولة من جهة، وبين إدارات الدولة ومؤسساتها الإدارية العامة من جهة أخرى لأغراض القيام بمهامها بدون رسوم[1]، وبذلك وضع المشرع نشر قرارات وأحكام المحاكم في إطار عام للبيانات العامة المفتوحة لضمان وصول المواطنين بطريقة أفضل إلى المؤسسة القضائية، وهو ما يفتح الطريق إلى اكتشاف دور الذكاء الاصطناعي في دعم اتخاذ القرار القضائي.

كما حرص المشرع الإماراتي على أن يتخذ لتقنيات الذكاء الصناعي مكانًا عليّا في أنظمة المحاكمات القضائية، من خلال إصداره عدداً من التشريعات التي جعلت من تلك التقنيات وسائل تستطيع بها المحاكم الوطنية بل وعبر الوطنية اتخاذ القرار القضائي الصحيح في ضوء ما يتوفر لديها من معلومات وبيانات عن المتهمين في القضايا المعروضة عليها، وهو ما سيتم تناوله في التقسيم التالي:

الفرع الأول: صور تقنيات الذكاء الاصطناعي في دعم اتخاذ القرار القضائي

الفرع الثاني: موقف المشرع الإماراتي من دعم اتخاذ القرار القضائي عبر تقنيات الذكاء الاصطناعي

(1)Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, dite « Lemaire », JORF n°0235 -consulté le 30/12/2020 www.legifrance.gouv.fr/

الفرع الأول

صور تقنيات الذكاء الاصطناعي في دعم اتخاذ القرار القضائي

تتعدد صور تقنيات الذكاء الاصطناعي التي يمكن الاستعانة بها في دعم القرار القضائي، فهي حاضرة وبقوة في أتمتة السوابق القضائية، وفي إمكانية سماع الشهود من معاقي السمع أو النطق، كما أن لهذه التقنيات دور مهم في تقدير التعويضات الناشئة عن الجرائم، وكذلك في سرعة الفصل في القضايا الجنائية، على التفصيل التالي:

أولًا: دور الذكاء الاصطناعي في أتمتة السوابق القضائية:

إن المهمة الأولى التي من المهم تكليف خوارزميات الذكاء الاصطناعي بها هي مساعدة القاضي أثناء التحقيق في القضية مستفيدًا من المعرفة العامة بالقضايا والأحكام والسوابق الصادرة عن المحاكم في هذا الشأن، والمقصود من دعم القرار القضائي هو مساعدة القاضي بأدوات آلية دون اتخاذ القرار نيابة عنه، بإتاحة قواعد البيانات وأدوات الكمبيوتر التفاعلية لاستخراج مجموعة من الحالات المشابهة للحالة محل البحث على أفضل وجه (النصوص القانونية المطبقة، الوقائع، الجريمة، التهمة ... إلخ) لاستخراجها من تلك القاعدة التي تشبهها وفقًا لهذه المعايير، يمكن أيضًا أن يُعهد بعمل الاستخراج هذا إلى خوارزمية مشتقة من الذكاء الاصطناعي يكون هدفها تحديد تصنيف للحالات المسجلة في قاعدة البيانات دون إعطاء نفسها أي معايير تصفية أو تصنيف مسبقًا وتزويد القاضي بمجموعة من القضايا "بشكل تلقائي" قريبة من تلك المعروضة أمامه للحكم فيها، دون أن يضطر إلى تحديد المعايير المشابهة بنفسه[1]. ويوجد العديد من هذه المواقع المفتوحة البيانات للكافة والتي تساعد عبر تقنيات البحث في الوصول إلى السوابق القضائية بسهولة، ومن ثم تمثل مصدرًا لتعليم المتقاضين السوابق القانونية من جهة، واستدعاء تلك السوابق في معاونة القضاة على الإسراع في الفصل في القضايا من جهة أخرى[2].

بيد أنه استنادًا إلى البيانات التي ينتجها الذكاء الاصطناعي، هل يمكن أن تقود "الأداة التنبؤية" إلى الاعتقاد بأن القاضي سيتعين عليه الحكم بما كشفت عنه نتائج هذه السوابق القضائية من الخوارزمية ذات الصلة، هذا قد يتعارض مع مبدأ تفريد العقوبة، حيث إن العقوبة شخصية، كما أن الأعذار والظروف القانونية المخففة وأدوات القاضي في وقف تنفيذ العقوبة أو الإعفاء منها

(1) Laurence Pécaut-Rivolier et Stéphane Robin, Référence précédente.

(2) مثال موقع محكمة النقض المصرية www.cc.gov.eg، وموقع محكمة النقض الفرنسية www.courdecassation.fr، وموقع دائرة القضاء بإمارة أبو ظبي www.adjd.gov.ae، وموقع محكمة التمييز بإمارة دبي www.dc.gov.ae.

هي من الثوابت القانونية، لذلك يجب على القاضي أن يصدر حكمه دومًا على أساس العناصر الموضوعية للمتهم (كالمهنة، الرعاية الطبية والاجتماعية، الوضع الأسري، المالي، العمر، السوابق الإجرامية .....إلخ) وفق المفهوم الإنساني للعدالة الجنائية الذي لن يكون متوفراً في "القرار الخوارزمي".

ويُثار التساؤل هل يمكن أن يحل تقييم خطر العودة إلى الإجرام بواسطة الأدوات التنبؤية في الإجراءات الجنائية محل العوامل السابقة؟ وهل مراعاة البيانات المعروفة من ماضي الجاني تجعل من الممكن بناء مشروع لإعادة دمجه في المستقبل تحت ستار تعزيز مبدأ المساواة بين المواطنين أمام القانون، ربما يحدث ذلك، علمًا بأن كلمة "ربما" هنا مهمة، حيث إن الأسلوب التجريبي ليس وسيلة مؤكدة للوصول إلى الهدف المنشود، ويبدو هذا الخوف معقولاً في الواقع، ما لم يتم النظر إلى الذكاء الاصطناعي من منظور التكامل وليس التبعية لمنصب القاضي الجنائي الذي لن يسمح للذكاء الاصطناعي في تقويض مبدأ التفريد، لأنه قطعًا سيسترشد بروحه وضميره في تفريد العقوبة من خلال إدراك التحيزات التي قد تكون متأصلة في الأدوات "التنبؤية".

ثانيًا: دور الذكاء الاصطناعي في سماع الشهود معاقي السمع أو النطق:

لا يمكن إنكار قوة الذكاء الاصطناعي في التوصل إلى تقنيات تستفيد منها العدالة وأطراف الدعوى الجنائية إذا كانوا من المجني عليهم أو الشهود أو غيرهم من معاقي السمع أو النطق، ويستخدمون لغة الإشارة للتواصل، أو يعتمدون على صديق أو قريب لتفسير هذه الإشارات نيابة عنهم لهيئة المحكمة، حيث تم استحداث قفاز ذكي يتيح لمستخدمي لغة الإشارة التواصل مع الآخرين بدون مساعدة مترجم، وهذا القفاز مزود بقائمة محددة مسبقًا من مفردات لغة الإشارة، وبارتدائه واستخدام لغة الإشارة يترجم القفاز حركات أيديهم إلى حديث بإدراج خوارزمية تعليم آلية في تصميم القفاز تجعله يتعلم من الإشارات الخاصة بالمستخدم، بحيث يمكن لكل مستخدم تدريب قفازه على حركاته واستحداث قائمة من الإشارات مكيفة حسب احتياجاته.

كما أن هذا القفاز مزود بأجهزة استشعار متعددة لقياس حركات اليد الفردية للشخص وتتبعها وتسجيلها، ومصحوب بتطبيق يتيح التعبير عن الحركات في صورة نص و/أو حديث. ويمكن أيضًا للمستخدمين اختيار لغة القفاز (مثال الإنجليزية والفرنسية والعربية)، والصوت (مثال: ذكر وأنثى أو طفل) الذي يريدون أن يعبروا به. فالقفاز يترجم الحركات إلى نص مكتوب يظهر على شاشة الإسورة ثم يحولها إلى صوت يخرج من مكبر صوت صغير موضوع أيضًا على الإسورة. فحين يستخدم التطبيق يظهر النص المكتوب على شاشة جهاز ذكي مزدوج الاستخدام ويتحول إلى صوت يخرج من خلال مكبرات صوت الجهاز. فالقفاز هو في الواقع نظام اتصال ثنائي الاتجاه حيث يتيح لمن يعانون من إعاقات سمعية أو نطقية التواصل بشكل مستقل ومباشرة مع الآخرين بدون مترجم[1]. وهو ما يجعل هؤلاء قادرين على التعبير عن شهاداتهم التي تدعم المحكمة الجنائية في الوصول للحقيقة، والحكم بما يستقر عليه يقينها.

ثالثًا: دور الذكاء الاصطناعي في تقدير التعويضات الناشئة عن الجرائم:

تتمثل المهمة الأكثر طموحًا بلا شك في اقتراح قرار على القاضي بشأن القضية التي يجب أن يتعامل معها، فمثلًا فيما يتعلق بالدعوى المدنية أمام المحكمة الجنائية للمطالبة بالتعويضات المطلوبة عن الأضرار التي خلفتها الجريمة للمجني عليه أو ورثته[2]، ففي حالة عدم وجود معيار ملزم فقد نرغب في استخدام الذكاء الاصطناعي للتنبؤ بالتعويض العادل عن الأضرار التي نشأت من جريمة معينة، بناءً على قاعدة بيانات مكونة من السوابق القضائية، فهنا مرة أخرى يمكن للقاضي أن يحتفظ بالسيطرة على هذه العملية من خلال تحديد المعايير التي يعتبرها ذات صلة لاستخراج مواقف أو قضايا مشابهة لتلك التي يجب أن يتعامل معها، وبالتالي الحصول على مجموعة من البدائل التي تتفق مع الطلب المعروض عليه في القضية، كما ويمكن اللجوء إلى خوارزمية التعلم من أجل إنشاء "معادلة تنبؤ" مرتبطة بوصف كل حالة للحصول على اقتراح بتعويض أقرب ما يمكن إلى التعويض الذي تم منحه بالفعل في حالات مشابهة، ويكفي عندئذٍ تقديم دراسة القضية المطروحة لهذه الصيغة للحصول على تنبؤ بالتعويض "الجيد"[3].

رابعًا: دور الذكاء الاصطناعي في سرعة الفصل في القضايا الجنائية:

ربما يكون بطء صدور الأحكام القضائية أحد أقوى الانتقادات الموجهة إلى القضاء في أدبيات معظم العصور والدول، لأن العدالة بطيئة بطبيعتها، حيث إن مصداقيتها تقوم على احترام إجراءات ومواعيد وضمانات كفالة الحق في الدفاع في الخصومة الجنائية، وهو ما قد يستغرق وقتًا طويلًا، ومن بين الأسباب الرئيسة للبطء هي وسائل العدالة ذاتها، ولا سيما عدد القضايا لكل قاضٍ وكاتب، وفي هذا السياق يُعد استخدام الذكاء الاصطناعي أملًا في تسريع العمل القضائي، لتحسين الاستجابة الكمية لعدد القضايا التي يتم متابعتها، إما بتبسيط معالجة الإجراءات في المراحل

(1) Wipo Magazine - BrightSign: a smart glove that gives a voice to those who cannot speak – Availabe on line on 06/01/2021 at BrightSign: a smart glove that gives a voice to those who cannot speak (wipo.int)

(2) تنص المادة 22 فقرة 1 من قانون الإجراءات الجزائية الاتحادي الإماراتي على أنه "لمن لحقه ضرر شخصي مباشر من الجريمة أن يدعي بالحقوق المدنية قبل المتهم أثناء جمع الاستدلالات أو مباشرة التحقيق أو أمام المحكمة التي تنظر الدعوى الجزائية ..... إلخ".

(3) Laurence Pécaut-Rivolier et Stéphane Robin, Référence précédente.

الأولى، أو السماح بالاستجابة السريعة للحالات التي تعتبر "جماعية" أو لا تحتاج في الغالب إلى تحقيق جنائي مستقل، مثل مخالفات المرور[1].

ويقدم بعض الفقه مقترحات ناجعة في هذا المجال كمحاولة لمعالجة ظاهرة قضايا الشيك بدون رصيد التي أصبحت في تزايد مستمر في دولة الإمارات العربية المتحدة، مما أثقل كاهل الجهات الأمنية والقضائية في التعامل معها، وهو الأمر الذي أدى في النهاية إلى أن شغلت هذه الجريمة حيزًا لا يستهان به من وقت، وعمل، وجهد الجهات المعنية، حيث وصلت على سبيل المثال في إمارة دبي إلى 38% من حجم العمل اليومي بمراكز الشرطة، والنيابة العامة، والقضاء.

وعلى ذلك يمكن توضيح أن الإشكالية الرئيسية تكمن في عدم تناسب الإجراءات الجزائية التقليدية مع جرائم الشيك بدون رصيد، بما يترتب عليه ضرورة البحث في بدائل إجرائية مناسبة تحقق التوازن بين أغراض الإجراء الجنائي، ومراعاة حقوق المتهم، وتحقيق سرعة الفصل في القضايا الجنائية التي لا تحتاج بحسب طبيعتها للإجراءات التقليدية، وحيث إن هناك علاقة تبادل منفعة بين القانون والذكاء الاصطناعي، إذ يساعد الذكاء الاصطناعي وتطبيقاته على تخفيف الأعباء عن المتقاضين، لذلك اقترح هذا الفريق توفير نظام قانوني إلكتروني من شأنه الربط بين جهة تلقي البلاغات، وضبطها)الشرطة والجهات القضائية المعنية) بالإضافة إلى البنوك في حالة قضايا الشيكات المرتجعة، وبين كل من النيابة العامة والمحكمة المختصة، بحيث إذا تلقت الشرطة بلاغًا في أي من هذه الجرائم، فإن أدلة ثبوتها تكون قطعية، وبالتالي لا تحتاج إلى تحقيق ابتدائي من النيابة العامة التي تتولى إحالتها في الأوضاع العادية بدون تحقيق مباشرة من خلال رسالة نصية إلكترونية تشتمل على محضر الضبط والأدلة إلى المحكمة الجنائية المختصة المنعقدة إلكترونيًا دائمًا والمكونة من قاضٍ واحد، بحيث يتلقى القاضي هذه الرسالة، ويكون بإمكانه خلال دقيقة واحدة النظر في القضية وإصدار الحكم المناسب لها، والذي يكون في جميع الأحيان دائرًا حول عقوبة الغرامة [2].

كما يمكن استخدام الذكاء الاصطناعي في القضايا التي يتم فيها الدفع بانقضاء الدعوى الجنائية لسابقة الفصل فيها، فإذا كان المعروض على المحكمة ذات الوقائع والمتهمين في دعوى سبق الفصل فيها بحكم بات فهنا لا يجوز للقاضي الجنائي – بقوة القانون - إصدار أي حكم جديد

(1) Laurence Pécaut-Rivolier et Stéphane Robin, Référence précédente.

(2) عميد دكتور/ غيث غانم سيف السويدي – مدير أكاديمية شرطة دبي – دور الذكاء الاصطناعي في تبسيط إجراءات التقاضي –دراسة قانونية تطبيقية على جريمة الشيك بدون رصيد "مقترح قضية الدقيقة الواحدة" – دراسة منشورة بمجلة القضاء والقانون – دائرة القضاء – السنة السابعة العدد 8 - أكتوبر 2020 – صـ 41 وما بعدها.

يناقض قوة الأمر المقضي به في الحكم السابق[1]، إلا أن الاستجابة لهذا الدفع يتوقف على صحته، وهذا يتطلب من المحكمة فحص أوراق الدعوى المعروضة عليها، وتلك السابقة عليها، للتحقق من مدى مطابقة الشروط القانونية سالفة البيان في إطارها الواقعي والقانوني، وهنا على القاضي – في كل حالة على حدة – أن يتأكد مما سلف، لاستخلاص النتائج وفقًا لخصوصية كل قضية. يمكن أن يساعد الذكاء الاصطناعي في هذا العمل، من خلال توفير قواعد بيانات كاملة وأنظمة بحث فعالة تسمح للقضاة بالاستفادة من الأدوات التشغيلية لإنجاز مهمتهم في أسرع وقت ممكن ولأكبر عدد من القضايا في مثل تلك الحالات[2].

الفرع الثاني
موقف المشرع الإماراتي من دعم اتخاذ القرار القضائي عبر تقنيات الذكاء الاصطناعي

تتبوأ الحداثة القانونية لدى المشرع الإماراتي مكانًا عليًا، فهو يولي اهتمامًا فريدًا بالتشريعات التي تُعنى بتقنيات الذكاء الاصطناعي دعمًا لاتخاذ القرار القضائي المؤسس على البيانات والمعلومات ذات الموثوقية العلمية المستخرجة من هذه التقنيات، والتي تستوي في حجيتها مع تلك الأدلة المادية، حيث أصدر عددًا من القوانين في هذا الإطار يستطيع كاتب هذه السطور رصدها من خلال ما يلي:

أولًا: قانون المشروعات ذات الصفة المستقبلية:

أصدر المشرع الاتحادي المرسوم بقانون اتحادي رقم 25 لسنة 2018 صادر بتاريخ 2018/09/23م. الموافق فيه 13 محرم 1440هـ. بشأن المشروعات ذات الصفة المستقبلية[3]، حيث خَوّل في مادته الأولى مجلس الوزراء بمنح ترخيص مؤقت لتنفيذ أي مشروع مبتكر قائم على تقنيات حديثة ذات صفة مستقبلية أو باستخدام الذكاء الاصطناعي ولا يوجد تشريع منظم له في الدولة، وذلك بهدف إعداد تشريع منظم لنشاط المشروع في الدولة، ولمجلس الوزراء في سبيل ذلك وضع الشروط

(1) تنص المادة 20 فقرة 1 من قانون الإجراءات الجزائية الاتحادي الإماراتي على أنه "تنقضي الدعوى الجزائية بوفاة المتهم أو بصدور حكم بات فيها ....."، كما تنص المادة 268 فقرة 1 من ذات القانون على أنه "تنقضي الدعوى الجزائية بالنسبة للمتهم المرفوعة عليه والوقائع المسندة فيها إليه بصدور حكم بات فيها بالبراءة أو الإدانة".

(2) Laurence Pécaut-Rivolier et Stéphane Robin, Référence précédente.

(3) صدر المرسوم بقانون اتحادي رقم 25 لسنة 2018صادر بتاريخ 23/09/2018م.الموافق فيه 13 محرم 1440هـ. بشأن المشروعات ذات الصفة المستقبلية بتاريخ 23 من سبتمبر 2018 والمنشور في عدد الجريدة الرسمية رقم 638 ملحق صفحة 9.

والضوابط والإجراءات اللازمة لترخيص تلك المشروعات وتنفيذها، واستثنائه من أي تشريع اتحادي في الحدود التي تقتضي تنفيذ المشروع وذلك لفترة زمنية مؤقتة.

وبناءً عليه صدر قرار مجلس الوزراء رقم 14 لسنة 2019 بتاريخ 2019/01/29م.في شأن تنظيم إصدار التراخيص المؤقتة للمشاريع المبتكرة ذات الصفة المستقبلية[1] الذي عرّف المشروع المبتكر بأنه "أي مشروع يتم تطبيقه بتقنيات حديثة ذات صفة مستقبلية أو باستخدام أدوات الذكاء الاصطناعي، ولا يوجد تشريع منظم له في الدولة، وقد حددت مادته الثانية شروط الترخيص المؤقت للتشريعات المبتكرة، كما حددت مادته الثالثة إجراءات منح هذه التراخيص، بينما وبموجب مادته الخامسة تم إنشاء ما يسمى "مختبر التشريعات" ليتولى عدداً من المهام من بينها تعزيز دور الدولة الريادي في مجال التشريعات ذات الصفة المستقبلية، واقتراح التشريعات التي تقنن تطبيق المشاريع المبتكرة ذات الصفة المستقبلية بالتعاون مع الجهات الحكومية والخاصة والمختصين.

ثانيًا: دور تقنيات الذكاء الاصطناعي في قانون حماية البيانات الشخصية[2]:

أصدر المشرع الإماراتي المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية الذي عرفت مادته الأولى البيانات بأنها "مجموعة منظمة أو غير منظمة من المعطيات أو الوقائع أو المفاهيم أو التعليمات أو المشاهدات أو القياسات تكون على شكل أرقام أو حروف أو كلمات أو رموز أو صور أو فيديوهات أو إشارات أو أصوات أو خرائط أو أي شكل آخر يتم تفسيرها أو تبادلها أو معالجتها عن طريق الأفراد أو الحواسيب وتشمل المعلومات أينما وردت في هذا المرسوم بقانون.

بينما عرفت ذات المادة البيانات الشخصية بأنها "أي بيانات تتعلق بشخص طبيعي محدد أو تتعلق بشخص طبيعي يمكن التعرف عليه بشكل مباشر أو غير مباشر من خلال (الربط بين البيانات) من خلال استخدام عناصر التعريف كاسمه أو صوته أو صورته أو رقمه التعريفي أو المعرف الإلكتروني الخاص به أو موقعه الجغرافي أو صفة أو أكثر من صفاته الشخصية أو الفسيولوجية أو الاقتصادية أو الثقافية أو الاجتماعية، وتشمل البيانات الشخصية الحساسة والبيانات الحيوية البيومترية".

والبيانات الشخصية الحساسة كما هي مُعرفة بذات المادة هي "أي بيانات تكشف بشكل مباشر أو غير مباشر عن عائلة الشخص الطبيعي أو أصله العرقي أو آرائه السياسية أو الفلسفية أو معتقداته الدينية أو سجل السوابق الجنائية الخاصة به ...".

بينما البيانات الحيوية البيومترية هي تلك البيانات الشخصية الناتجة عن المعالجة باستخدام تقنية محددة تتعلق بالخصائص الجسدية أو الفسيولوجية أو السلوكية لصاحب البيانات والتي تسمح بتحديد أو تؤكد التحديد الفريد لصاحب البيانات مثل صورة الوجه أو بيانات البصمة. وهو ما يؤكد دور تقنيات الذكاء الاصطناعي في الوصول للجناة تحقيقًا للعدالة الجنائية.

ولغايات إنجاز مهام العمليات محل هذا القانون والتي تتم عبر تقنيات الذكاء الصناعي المؤتمتة، فقد عرف المشرع المعالجة المؤتمة بأنها "المعالجة التي تتم باستخدام برنامج أو نظام إلكتروني يعمل بطريقة آلية وتلقائية إما بشكل مستقل كليًا دون أي تدخل بشري أو بشكل جزئي بإشراف وتدخل بشري محدود".

ومن أحد أشكال تلك المعالجة المؤتمتة ما يسمى في هذا التشريع بـ "التنميط"، حيث تتضمن استخدام البيانات الشخصية لتقييم جوانب شخصية معينة ومرتبطة بصاحب البيانات ومن بينها تحليل أو توقع الجوانب المتعلقة بأدائه أو وضعه المالي أو صحته أو تفضيلاته الشخصية أو اهتماماته أو سلوكه أو مكانه أو تحركاته أو موثوقيته، وهو ما يعكس أهمية التنميط كأحد أشكال الذكاء الاصطناعي في الكشف عن الجناة، أو حتى رسم ملامح التوقعات حول احتمالية ارتكاب شخص ما لجريمة مستقبلًا.

وتحدد المادة الثانية نطاق سريان هذا القانون على معالجة البيانات الشخصية سواءً كلها أو جزء منها عن طريق وسائل الأنظمة الإلكترونية التي تعمل بشكل تلقائي وآلي، كما تحدد المادة الرابعة حالات معالجة البيانات الشخصية بدون موافقة صاحبها، حيث تعتبر المعالجة مشروعة في عدد من الحالات من بينها ما ورد بالفقرة (3) أن تكون المعالجة ضرورية لإقامة أي من إجراءات المطالبة بالحقوق والدعاوى القانونية أو الدفاع عنها أو تتعلق بالإجراءات القضائية أو الأمنية.

كما لا يحق لصاحب البيانات طلب محو بياناته الشخصية إذا كان هذا المحو يؤثر على إجراءات التحقيق والمطالبة بالحقوق والدعاوى القانونية أو الدفاع عنها لدى المتحكم[1] الذي عرفته المادة الأولى بأنه "المنشأة أو الشخص الطبيعي الذي لديه بيانات شخصية وبحكم نشاطه يقوم بتحديد طريقة وأسلوب ومعايير معالجة هذه البيانات الشخصية والغاية من معالجتها سواءً بمفرده أو بالاشتراك مع أشخاص أو منشآت أخرى".

كما يحق لصاحب البيانات أن يطلب من المتحكم الاستمرار بالاحتفاظ ببياناته الشخصية لما

(1) صدر قرار مجلس الوزراء رقم 14 لسنة 2019 صادر بتاريخ 2019/01/29م.الموافق فيه 13 محرم 1440هـ. في شأن تنظيم إصدار التراخيص المؤقتة للمشاريع المبتكرة ذات الصفة المستقبلية بتاريخ 29 يناير 2019 والمنشور في عدد الجريدة الرسمية رقم 647 صفحة 739.

(2) صدر المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية بتاريخ 20 سبتمبر 2021 والمعمول به اعتبارًا من 2 يناير 2022.

(1) راجع المادة (15) فقرة 3 من المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية.

بعد انتهاء أغراض المعالجة كون هذه البيانات ضرورية له لاستكمال إجراءات متعلقة بالمطالبة بالحقوق والدعاوى القضائية أو الدفاع عنها، ورغم ذلك فللمتحكم المضي قدمًا في معالجة البيانات الشخصية لصاحبها دون موافقته إذا كانت ضرورية لإقامة أي من إجراءات المطالبة بالحقوق والدعاوى القانونية أو الدفاع عنها أو تتعلق بالإجراءات القضائية [1].

وإذ يحق لصاحب البيانات الاعتراض على القرارات التي تصدر عن المعالجة (المؤتمتة) وتكون لها تبعيات قانونية أو تؤثر بشكل جسيم على صاحب البيانات بما فيها التنميط الذي يمكن من خلاله تحليل أو توقع الجوانب المتعلقة بأدائه أو وضعه المالي أو سلوكه أو مكانه أو تحركاته أو موثوقيته كما سلف بيانه، وهو ما يبرز معه دور الذكاء الاصطناعي في هذا المجال، إلا انه لا يجوز لصاحب البيانات – وقد يكون متهمًا في إحدى القضايا الجنائية - الاعتراض على تلك القرارت إذا كانت تلك المعالجة المؤتمتة ضرورية وفق تشريعات أخرى نافذة في الدولة، ومنها بالطبع تشريعات الجرائم والعقوبات والإجراءات الجزائية والتشريعات الجنائية الخاصة، إلا أنه من المحتمل أن يشوب الخطأ تلك المعالجات المؤتمتة - بما فيها التنميط – التي تستخدم فيها تقنيات الذكاء الاصطناعي، لذلك فقد أوجب القانون على المتحكم إدخال "العنصر البشري" في مراجعة قرارات المعالجة المؤتمة بناءً على طلب صاحب البيانات [2].

ولغايات طبيعة بعض الجرائم العابرة للحدود، وما يشكله ذلك من وجود بعض الجناة خارج النطاق الجغرافي للدولة، وما توجبه بعض الاتفاقيات المتعلقة بالتعاون القضائي الدولي فقد أجاز المشرع الإماراتي نقل تلك البيانات الشخصية إلى خارج الدولة إذا كان هذا النقل ضرورياً لتنفيذ التزامات وإثبات الحقوق أمام الجهات القضائية أو ممارستها أو الدفاع عنها، أو تنفيذًا لإجراء متعلق بتعاون قضائي دولي [3].

ثالثًا: دور تقنيات الذكاء الاصطناعي في قانون مكافحة الشائعات والجرائم الإلكترونية:

حرص المشرع الإماراتي على تأثيم استخدامات الذكاء الاصطناعي في ارتكاب بعض الجرائم المنصوص عليها في المرسوم بقانون مكافحة الشائعات والجرائم الإلكترونية [4] حيث عرفت مادته

(1) راجع المادة (16) فقرة 2 و3 بند (ب) من المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية.

(2) راجع المادة (18) فقرة 1 و2 - ب و4 من المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية.

(3) راجع المادة (23) فقرة 1 بند ج -هـ من المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية.

(4) صدر المرسوم بقانون اتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية بتاريخ 20 من سبتمبر 2021 والنافذ اعتبارًا من 02 من يناير 2022.

الأولى الروبوت الإلكتروني وهو أحد استخدامات الذكاء الاصطناعي بأنه "برنامج إلكتروني يتم إنشاؤه أو تعديله لغرض تشغيل المهام المؤتمتة بكفاءة وسرعة"، ولغايات هذا التعريف عاقب المشرع بالحبس مدة لا تزيد على سنتين والغرامة التي لا تقل عن مائة ألف درهم ولا تزيد على مليون درهم أو بإحدى هاتين العقوبتين كل من أنشأ أو عدل روبوتاً إلكترونياً بقصد نشر أو إعادة نشر أو تداول بيانات أو أخبار زائفة في الدولة أو تمكين الغير من نشرها أو إعادة نشرها أو تداولها، وتشدد العقوبة عند تعدد الجناة، وفق ما نصت عليه المادة 54 من ذلك القانون.

كما أسبغت المادة الثالثة عشرة من ذات المرسوم بقانون التأثيم على كل من استخدم تقنية المعلومات أو إحدى وسائل تقنية المعلومات لجمع أو حفظ أو (معالجة) بيانات ومعلومات شخصية للمواطنين أو المقيمين بالدولة بالمخالفة للتشريعات النافذة في الدولة، حيث يعاقب مرتكبو هذه الجرائم بالحبس والغرامة التي لا تقل عن خمسين ألف درهم ولا تزيد على خمسمائة ألف درهم أو بإحدى هاتين العقوبتين. جدير بالذكر أن البيانات والمعلومات الشخصية كما هي معرفة بنص المادة الأولى من ذات المرسوم بقانون هي تلك الخاصة بالأشخاص الطبيعيين متى كانت مرتبطة بحياتهم الخاصة أو تحدد هويتهم أو يمكن من خلال ربط هذه المعلومات والبيانات بطريقة مباشرة أو غير مباشرة تحديد ومعرفة (هوية الشخص).

ولا جدال في أن تقنيات الذكاء الاصطناعي المؤتمتة تعتمد في تشغيلها على الأجهزة الإلكترونية ونظم المعلومات وبرامج الحاسب ووسائل تقنية المعلومات، وقد يحتج المتهم أمام جهات إنفاذ العدالة بعدم موثوقية الأدلة المستخرجة من هذه التقنيات، لذلك حرص المشرع الإماراتي في المادة (65) من ذات المرسوم بقانون التي صدرت تحت عنوان (حجية الأدلة)، على أن "يكون للأدلة المستمدة أو المستخرجة من الأجهزة أو المعدات أو الوسائط أو الدعامات الإلكترونية أو النظام المعلوماتي أو برامج الحاسب أو من أي وسيلة لتقنية المعلومات حجية الأدلة الجنائية المادية في الإثبات الجنائي".

خلاصة ما سلف يتضح منه مدى اهتمام المشرع الإماراتي بتقنين دور تقنيات الذكاء الاصطناعي لدعم اتخاذ القرارا القضائي، وتحقيقًا للعدالة الجنائية وإنفاذ القانون، من خلال التشريعات سالفة البيان التي تتسم بوضوح نصوصها، ودقة صياغتها، وجمال تعبيراتها، وكمال تنسيقها، وحسن ترتيبها، تتميز في ذلك بطابعها العلمي والمنطقي الذي يحقق الانسجام بين القانون والواقع الحاضر بل والمستقبل، وبما يكفل تحقيق العدالة من جهة والموازنة بين المصالح المختلفة من جهة أخرى.

المطلب الثاني

دور الذكاء الاصطناعي في تطوير السياسات العقابية وتأكيد اليقين القانوني

بالتزامن مع التطورات التقنية في مجال التكنولوجيا الحديثة فتحت متطلبات العدالة العقابية أبوابًا أمام فلسفة جديدة تسمى ببدائل العقوبات أو التدابير السالبة للحرية لم يكن لها وجود لولا تطور تقنيات الذكاء الاصطناعي، حيث أصبح بالإمكان استخدامها في مجال المراقبة الإلكترونية للمتهمين أو المحكوم عليهم كبديل للحبس الاحتياطي أو العقوبات السالبة للحرية قصيرة المدة أو الإفراج المشروط في بعض الحالات التي يحددها المشرع لاعتبارات اجتماعية أو مهنية أو غيرها.

والمراقبة الإلكترونية هي حرمان المتهم أو المحكوم عليه من أن يتغيب في غير الأوقات الزمنية المحددة له عن محل إقامته أو أي مكان آخر يعينه الأمر الصادر من النيابة العامة أو المحكمة المختصة بحسب الأحوال، ويتم تنفيذه عن طريق "وسائل إلكترونية تسمح بالمراقبة عن بُعد" وتلزم الخاضع لها بحمل جهاز إلكتروني مدمج طوال فترة الوضع تحت المراقبة [1]. ويعتبر السوار الإلكتروني هو الوسيلة الأكثر شيوعًا حيث تعتمد على وضع جهاز إلكتروني صغير أشبه بساعة اليد حول المعصم ولا يمكن التقاطه أو اختلاطه بأجهزة أخرى، ويحمل رقماً خاصاً به، ويقوم بإرسال موجات في حدود مساحة معينة، فإذا ما تجاوزها الخاضع للمراقبة يرسل السوار إشارة تنبيه إلى مركز المراقبة والمتابعة مؤداها قرينة قد لا تقبل إثبات العكس لمخالفته للالتزامات الواردة بأمر الوضع تحت المراقبة الإلكترونية وقد ينتج عنها إلغاء هذا الأمر، ومن ثم العودة لحبس المتهم احتياطيًا أو تنفيذ العقوبة السالبة للحرية[2]، لعدم صلاحية هذا الشخص للاستفادة من مميزات هذه السياسة العقابية.

بيد أن استخدام الخوارزميات على هذا النحو يحد من تأثير اليقين القانوني أو التأكد من ارتكاب المخالفة الجنائية من عدمه، فقد يكون عطل هذا السوار أو عدم شحنه لخطأ أو غفلة أو سهو عن ذلك لبعض شأنه، ما أدى لتوقفه أو تلفه لا يجب أن يكون بذاته مؤشرًا للاستخدام الواسع للقرار "الخوارزمي" وجعل من نظام الذكاء الاصطناعي صانع القرار الرئيسي في إسناد المخالفة، بل يجب

(1) راجع المادة 355 من قانون الإجراءات الجزائية الاتحادي الإماراتي المضافة تحت عنوان "الإجراءات الجنائية الخاصة" بموجب المادة الثالثة من المرسوم بقانون اتحادي رقم 2018/17 بتاريخ 2018/09/23.

(2) راجع المادتين 376 و 379 من قانون الإجراءات الجزائية الاتحادي الإماراتي.

أن يكون فقط أداة مساعدة في بعض نواحي السياسة العقابية وإنفاذ القانون.

وعن دور تقنيات الذكاء الاصطناعي في تأصيل اليقين القانوني يقول البعض بأنها قد تكون ضمانة أساسية للمتقاضي تهدف إلى حمايته من تعسف بعض القضاة، ومن ثم تبني الدعوة إلى ترشيد القرار القضائي، والسماح بتوحيد أفضل لمعايير العدالة تأكيدًا لليقين القانوني، فالحق الذي لا يُطمأن إليه لن يكون حقًا، مُعللًا وجهة نظره بأن القرارات والأحكام القضائية بطبيعتها خاضعة للاختلاف من قاضٍ لآخر دون معيار أو سبب واضح لهذا الاختلاف رغم وحدة الظروف وتشابه الوقائع في العديد من الحالات، هذا التباين مرتبط بمدى علم القاضي وإحاطته وتفسيره للقاعدة القانونية، ومعتقداته وشخصيته، التي يمكن أن يكون لها تأثير لا إرادي على القرار أو الحكم القضائي، فقد أظهرت العديد من الدراسات أن العوامل المتنوعة للغاية والمفاجئة في بعض الأحيان - كوجبة إفطار القاضي، ومدى إرهاقه، وتأثير وسائل الإعلام عليه - يمكن أن تؤثر على القرار المتخذ أو الحكم المنطوق به[1]. لذلك يمكن للذكاء الاصطناعي تحسين هذه الوظيفة وطمأنة أولئك الذين يعتبرون أنه من الضروري أن يكون هناك عدالة تضمن وحدة هوية الحل القانوني في مفهوم الموثوقية على أساس المساواة واليقين، أي أن الحالة (أ) ستؤدي إلى الإجابة (ب) [2].

إن هذه الأسباب لاختلاف قرارات وأحكام المحكمة – في نفس الحالات – تؤدي إلى خطر اضطراب اليقين القانوني لدى العامة، وفي مواجهة هذا الخطر، توجد ضمانات متعددة كالرقابة الداخلية، والسوابق القضائية التي توحد تفسير النصوص، وهو ما دعا المشرع في العديد من الدول إلى تبني تعيين جهات قضائية تختص بتوحيد تفسير النصوص الدستورية والتشريعية لسلامة تطبيقها واستقرار المبادئ القانونية من جهة، وتأسيس دوائر قضائية تعمل على توحيد المبادئ القضائية التي تصدر عن المحاكم المختلفة من جهة أخرى[3].

(1) من خلال دراسة للفيلسوف الأمريكي والقاضي جيروم فرانك في عام 1950 نشرت في مجلة Proceedings الأكاديمية الوطنية للعلوم (PNAS) أن جوع أو شبع القاضي يؤثر على قراره، وقد نظر مؤلفو الدراسة في أكثر من 1000 قرار إفراج مشروط اتخذها ثمانية قضاة مختلفين خلال فترة عشرة أشهر، فمن 14 إلى 35 قضية يوميًا في ثلاث جلسات: واحدة من بداية اليوم إلى استراحة لتناول وجبة خفيفة في منتصف الصباح، والثانية من الاستراحة الصباحية إلى استراحة الغداء والثالثة من استراحة الغداء حتى في نهاية اليوم. وبشكل عام كان القضاة أكثر ميلًا لقبول طلبات الإفراج المشروط في بداية اليوم منه في النهاية، حيث تضاعفت فرص قبول الطلب عند نظر القضية في بداية الجلسة، كما وأن عدد القضايا التي كان على القاضي التعامل معها خلال جلسة واحدة أثرت بشكل كبير على قراراته، اتبع القضاة الثمانية الذين تمت دراستهم نفس النمط، ورفضوا ما مجموعه 64.2% من الطلبات.

(2) Laurence Pécaut-Rivolier et Stéphane Robin, Référence précédente.

(3) بموجب المادة 99 فقرة 4 من الدستور الإماراتي تختص المحكمة الاتحادية العليا بتفسير أحكام الدستور إذا ما طلبت إليها ذلك إحدى سلطات الاتحاد أو حكومة الإمارات، ويعتبر هذا التفسير ملزمًا للكافة. كما وبموجب المادة 14 وما بعدها من القانون الاتحادي رقم 10 لسنة 2019 بشأن تنظيم العلاقات القضائية بين السلطات القضائية الاتحادية والمحلية تم إنشاء هيئة قضائية تسمى "هيئة توحيد المبادئ

بيد أنه حيث تتمثل إحدى خصائص الخوارزميات التنبؤية التي يوفرها الذكاء الاصطناعي في أنها تعمل مثل الصناديق السوداء، أي أن صيغة التنبؤ معقدة ما يجعل "توقع التنبؤ" ليس بالأمر السهل، ومن ثم فإن استخدامه في الإطار القانوني قد يجعل المتقاضين ومحاميهم غير قادرين في الواقع على معرفة القاعدة المطبقة عليه، فهل الثقة في موضوعية الآلة كافية لتبرير الجهل الذي قد يقع فيه صاحب العلاقة بالقرار؟[1]

بالإضافة إلى ذلك، يجب ألا يؤدي استخدام خوارزميات الذكاء الاصطناعي في سياق المحاكمة الجنائية إلى إعاقة ممارسة حقوق الدفاع وافتراض البراءة المكفول بموجب الدستور[2]، حيث يلزم معالجة مسألة عدم التيقُّن بشأن مدى الحرص الواجب فيما يخص تصميم الطرائق الحسابية أو المسؤولية المحتملة عن سوء عمل نظام الذكاء الاصطناعي، وذلك مع عدم القدرة على التنبؤ بسلوكه وعدم السيطرة على استخدامه ولا على مدخلات البيانات التي قد تؤثر تأثيرًا مهماً عليه، فمن وجهة نظر تقنية قد يستحيل تبرير سبب اتخاذ نظام الذكاء الاصطناعي لقرار ما، لذا فإن الأطراف تجد نفسها، في حال وقوع الضرر، في فراغ استدلالي وقد لا تتمكن من تحديد المسؤولية بالنظر لغياب الأحكام المحددة في هذا الشأن[3].

وهذا يعني وفقًا للمجموعة الأوروبية للأخلاقيات أنه لم تعد أفعال تلك التطبيقات الناتجة عن الذكاء الاصطناعي واضحة في كثير من الأحيان، ولم تعد المراقبة البشرية لما تقوم به متوفرة، هذا هو الحال لأنه من المستحيل تحديد كيفية الوصول إلى النتائج خارج نطاق الخوارزميات الأولية. حيث يستند أداء أنظمة الذكاء الاصطناعي إلى البيانات التي تم استخدامها أثناء عملية التعلم، والتي قد لا تكون متوفرة أو يمكن الوصول إليها. وهكذا، التحيزات والأخطاء المدخلة في النظام تصبح متأصلة ومتجذرة فيه[4].

القضائية الاتحادية والمحلية" تختص بتوحيد المبادئ القضائية المتعارضة الصادرة عن محكمتين أو أكثر من المحاكم العليا في دولة الإمارات، والنظر في طلبات العدول عن المبادئ المقررة سابقًا، على أن تلتزم كافة السلطات القضائية الاتحادية والمحلية بمختلف درجاتها بالمبادئ التي تقررها الهيئة، ويكون مخالفة أي حكم قضائي لاحق لأي من هذه المبادئ سببًا من أسباب الطعن فيه بأب من الطرق المقررة قانونًا.

(1)Laurence Pécaut-Rivolier et Stéphane Robin, Référence précédente.

(2) تنص المادة (28) من الدستور الإماراتي على أن (العقوبة شخصية، والمتهم بريء حتى تثبت إدانته في محاكمة قانونية وعادلة، وللمتهم الحق في أن يوكل من يملك القدرة للدفاع عنه أثناء المحاكمة، ويبين القانون الأحوال التي يتعين فيها حضور محام عن المتهم).

(3) الجوانب القانونية للعقود الذكية والذكاء الاصطناعي – ورقة عمل مقدمة من تشيكيا إلى لجنة الأمم المتحدة للقانون التجاري الدولي – الدورة الحادية الخمسون – نيويورك 25 من يونيو – 13 يوليه 2018 – مطبوعات الجمعية العامة للأمم المتحدة – 960/A/CN.9 – صـ 3.

(4) ديريك دوبريز - الاتحاد الأوروبي يناقش القضايا القانونية المتعلقة بالذكاء الاصطناعي – مقال مترجم من موقع ديجينوميكا - منشور بمجلة معهد دبي القضائي – العدد العد 10 - السنة السابعة - مارس 2019 - صـــ 148

لذلك فمن الضروري ضمان وصول الطرف المعني إلى البيانات التي يستخدمها الذكاء الاصطناعي من أجل تحدي أي استنتاجات خاطئة لأداة التنبؤ، كما يجب أن يكون مكفولاً صلاحية تشكيك أطراف المحاكمة في كل مرة يستخدم فيها القاضي الذكاء الاصطناعي لإصدار حكمه، حيث يجب السؤال عن كيفية وصول الخوارزمية إلى النتائج المطروحة، وهو ما قد يشعل الصراع بين أصحاب حقوق الملكية الفكرية من جهة، وحقوق الدفاع من جهة أخرى. فإذا أتيح هذا الحق في المعلومات سيحد من الآثار الضارة للذكاء الاصطناعي في تنفيذ الإجراءات الجنائية مع احترام مبدأ تكافؤ وسائل الدفاع وافتراض البراءة [1] وزياة اليقين القانوني للأطراف ذات الصلة.

لذلك تبنت المفوضية الأوروبية لكفاءة العدالة CEPEJ المبادئ الأساسية الخمسة التالية المسماة "الميثاق الأخلاقي الأوروبي لاستخدام الذكاء الاصطناعي في الأنظمة القضائية وبيئتها" [2]، هذا الميثاق موجه إلى الجهات العامة والخاصة المسؤولة عن التصميم ونشر أدوات وخدمات الذكاء الاصطناعي المتعلقة بمعالجة قرارات وبيانات المحاكم، كما أنها تهم صانعي القرار المسؤولين عن الإطار التشريعي أو التنظيم أو التطوير أو التدقيق أو استخدام هذه الأدوات والخدمات. إن الغرض من استخدام هذه الأدوات والخدمات في الأنظمة القضائية هو تحسين كفاءة وجودة العدالة بطريقة مسؤولة، مع استخدامها بأقصى قدر من التحفظات في المسائل الجنائية لمنع التمييز، وضمانًا للمحاكمة العادلة، وسواءً تم تصميمها بهدف تقديم الدعم للاستشارات القانونية، أو المساعدة في الصياغة أو اتخاذ القرار أو التوجيه للمتقاضين، حيث من الضروري أن تتم المعالجة المذكورة في ظل ظروف الشفافية والحياد، وهذه المبادئ هي:

المبدأ الأول: احترام الحقوق الأساسية Principe de respect des droits fondamentaux:

وذلك بضمان تصميم وتنفيذ أدوات وخدمات الذكاء الاصطناعي حين معالجة قرارات المحاكم والبيانات القضائية لتتوافق مع الحقوق الأساسية التي تضمنها الاتفاقية الأوروبية لحقوق الإنسان (ECHR) واتفاقية حماية البيانات الشخصية، مع التأكيد على أن استخدام أدوات الذكاء الاصطناعي في التقاضي أو كأداة للمساعدة في اتخاذ القرار أو التوجيه أمام القضاء يجب ألا تنتهك ضمانات الحق في المحاكمة العادلة بتعزيز الوصول إليها (تكافؤ وسائل الدفاع واحترام إجراءات الخصومة)، مع الاحترام الكامل لمبادئ سيادة القانون واستقلال القضاة في عملية صنع القرار.

(1) Camille Guillard - La justice prédictive et l'IA dans le procès pénal : risques et opportunités - Référence précédente.

(2) Charte éthique européenne d'utilisation de l'intelligence artificielle dans les systèmes judiciaires (coe.int), Référence précédente.

المبدأ الثاني: عدم التمييز Principe de non-discrimination:

على وجه التحديد منع خلق أو تعزيز أي تمييز بين الأفراد أو الجماعات، فيجب توخي الحذر في كل مراحل تطوير خوارزميات الذكاء الاصطناعي عندما تعتمد بشكل مباشر أو غير مباشر على البيانات "الحساسة" التي يمكن النظر فيها على الأصل العرقي أو الإثني، والظروف والآراء الاجتماعية والاقتصادية والسياسية والمعتقدات الدينية أو العضوية النقابية الفلسفية وكذلك البيانات الوراثية، والبيانات المتعلقة بالصحة أو المتعلقة بالحياة الجنسية أو التوجه الجنسي. حيث تهدف البيانات والمدخلات الصحيحة إلى الحد من أو تحييد مخاطر تمييز نتائج الخوارزمية.

المبدأ الثالث: الجودة والأمان Principe de qualité et sécurité:

فيما يتعلق بمعالجة قرارات المحاكم والبيانات القضائية يجب استخدام المصادر المعتمدة مع نماذج مصممة بطريقة متعددة التخصصات في بيئة تكنولوجية آمنة، وذلك بأن تجتمع خبرات مصممي نماذج خوارزميات التعلم الآلي مع ذوي الشأن من أفراد العدالة (القضاة والمدعين العامين والمحامين، وأساتذة القانون في الجامعات، والباحثين ..... إلخ) والباحثين، لإنتاج نماذج منظمة وظيفيًا لتحقيق أقصى استفادة من هذه التخصصات المتعددة، ويجب أن تأتي البيانات المستمدة من قرارات المحاكم والمدمجة في البرنامج الذي يدير خوارزمية التعلم الآلي من مصادر معتمدة وغير قابلة للتغيير حتى يتم استخدامها فعليًا بواسطة آلية التعلم، وبالتالي يجب أن تكون العملية برمتها قابلة للتتبع والتدقيق لضمان عدم حدوث أي تغيير يمكن أن يعدل محتوى أو معنى القرار الذي تتم معالجته، فضلًا عن وجوب حفظ وتشغيل النماذج والخوارزميات التي تم إنشاؤها في بيئة آمنة، مما يضمن تكامل النظام وعدم العبث أو المساس بها.

المبدأ الرابع: الشفافية والحياد والنزاهة الفكرية Principe de transparence, de neutralité et d'intégrité intellectuelle:

وذلك بجعل منهجيات معالجة البيانات مفهومة، والسماح بعمليات التدقيق الخارجية، حيث يجب إيجاد توازن بين حق منتج الخوارزمية في الملكية الفكرية لأساليب المعالجة، وبين متطلبات الشفافية التقنية الكاملة بإتاحة إمكانية الوصول إلى عملية التصميم، وحيث يكون ذلك مقيدًا بحقوق الملكية الفكرية وحماية الأسرار الصناعية، فيمكن أن يكون النظام الخوارزمي قابلًا للتفسير بلغة واضحة وشائعة للأطراف ذات العلاقة في العملية القضائية من أجل وصف الطريقة التي ينتج بها نتائجه من خلال بيان طبيعة الخدمات المقدمة، والأدوات التي تم تطويرها، ومخاطر الخطأ، هنا يمكن أن تكون السلطات أو الخبراء المستقلون مسؤولين عن تدقيق عمليات المعالجة

أو تقديم المشورة في المراحل الأولية، كما يمكن إصدار ملصقات متجددة بانتظام من قبل السلطات العامة. فضلًا عن وجوب التمتع بالحياد وعدم التحيز والنزاهة الفكرية حيث يتأثر التصميم وسلسلة التشغيل وجودة البيانات بأكملها بهذه التدابير.

المبدأ الخامس: التحكم والسيطرة من قبل المستخدم Principe de maîtrise par l'utilisateur:

يقتضي هذا حظر فرض نهج إلزامي والسماح للمستخدم بأن يكون فاعلًا ومستنيرًا وسيد اختياراته، فيجب تعزيز استقلالية المستخدم وعدم تقييده باستخدام أدوات وخدمات الذكاء الاصطناعي، كما يجب أن يكون المتخصصون القانونيون كالمحامين قادرين على الرجوع إلى الأحكام والبيانات القضائية التي تم استخدامها في خوارزميات الذكاء الاصطناعي للتأكد من نتيجتها، وإتاحة التخلي عنها في ضوء تفاصيل القضية المحددة، فضلًا عن إبلاغ المتقاضي بلغة واضحة ومفهومة بالطبيعة الملزمة للحلول التي تقترحها أدوات الذكاء الاصطناعي أم لا، والخيارات الممكنة المختلفة، وكذلك بحقه في المساعدة القانونية والاستئناف أمام المحكمة، ويجب أيضًا إبلاغ الخصم بوضوح بأي لجوء إلى المعالجة المسبقة للقضية بواسطة الذكاء الاصطناعي قبل أو أثناء العملية القضائية وأن يكون قادرًا على الاعتراض حتى يتم سماع قضيته مباشرة من قبل المحكمة، وبشكل عام يجب محو "الأمية الرقمية" للمستخدمين وطرح المناقشات التي يشارك فيها متخصصون قانونيون بمناسبة تنفيذ أي نظام معلومات قائم على الذكاء الاصطناعي.

الخاتمة:

قريبًا ستصبح تقنيات الذكاء الاصطناعي جزءًا رئيسًا من نظام العدالة الجنائية في جميع مراحله بدءًا من التنبؤ بالجرائم لمنع وقوعها مرورًا بكشفها والقبض على مرتكبيها بواسطة الأدلة التي تقدمها هذه التقنيات لأنظمة الشرطة، كما أسفرت هذه التقنيات عن مساهمة فعالة في تقديم العون لأطراف العدالة من أجهزة التحقيق والقضاة بل والمحامين لتقييم أدلة الدعوى الجنائية والتعويضات الناشئة عنها وصولًا للترضية القضائية بعد تحقق اليقين القانوني اللازم للحكم فيها من خلال هذه التقنيات.

النتائج:

أحرزت تقنيات الذكاء الاصطناعي تقدمًا مذهلًا يرجع الفضل فيه إلى تطور أبحاث التعلم الآلي التي أصبحت ممكنة مع استخدامها لكميات هائلة من البيانات الجنائية والقضائية التي كانت لها آثارٌ كبيرة على تطوير نظام العدالة الجنائية في مراحله المختلفة، وبما مهّد الطريق لمستقبل واعد للنظام القانوني.

جلبت تطبيقات الذكاء الاصطناعي تحديات منها مدى موثوقية جودة البيانات المستخدمة ومخرجات نتائجها، فالبيانات الرديئة تؤدي إلى نتائج رديئة، وهو ما قد يؤثر سلبًا على سلامة اليقين القانوني، مرورًا بالمخاطر الأمنية، وصولًا إلى انتهاكات الخصوصية وعوائق النفاذ العادل إلى منافع هذه التقنيات ونجاعة التعامل معها وتحليلها.

يقتصر دور هذه التقنيات على مساعدة أجهزة إنفاذ القانون والعدالة في اتخاذ القرار القضائي الصحيح إذا اعتمدت على بيانات ومعلومات صحيحة تساعد في الوصول للحقيقة وتحقيق اليقين القانوني، ولا يمكن أن تكون هذه التقنيات بديلًا عن القضاة الذين لهم وحدهم السلطة التقديرية في الحكم بالإدانة أو البراءة، وتطبيق الأعذار والظروف المخففة أو المشددة أو وقف تنفيذ العقوبة وفقًا لحالة كل متهم.

استطاع المشرع الإماراتي أن يقنن من التشريعات الحديثة ما يوثق به حجية مخرجات تقنيات الذكاء الاصطناعي دعمًا للقرار القضائي، ومساواتها بحجية الدليل المادي في الإثبات الجنائي، وذلك بصوغ تشريعات حماية البيانات الشخصية ومكافحة الجرائم الإلكترونية التي أصبحت ظهيرًا قانونيًا تليدًا لأجهزة إنفاذ القانون في الاعتماد على هذه التقنيات ومخرجاتها وصولًا للعدالة وتحقيقًا لها، مع تأصيل الخيارات القانونية للمتهمين في الاعتراض على أخطاء مخرجات هذه التقنيات التي – غالبًا - لا يتدخل فيها العنصر البشري.

التوصيات:

يأمل الباحث من البرلمانات التشريعية التأسّي بالقانون الإماراتي في سرعة صوغ إطار قانوني جديد للتشريعات الجنائية والقوانين الإجرائية ذات الصلة بتنظيم استخدام تقنيات الذكاء الاصطناعي تضمن احترام الحقوق الأساسية وجودة وأمان وحياد البيانات ذات الصلة بتحقيق العدالة الجنائية، وخضوعها لرقابة قضائية فعالة مع الأخذ في الاعتبار مخاطر تطبيقاته بما في ذلك تأثيرها على حقوق الدفاع وسيادة القانون.

يلفت الباحث نظر أجهزة الشرطة إلى أن استخدامات الذكاء الاصطناعي هي سلاح ذو حدين فقد يُمكّن الجماعات الإجرامية من الهجمات الإلكترونية، والاعتداءات الجسدية عن طريق الطائرات المُسيرة بدون طيار، ونشر الأخبار الكاذبة، فضلًا عن أدوات تغيير الوجوه والتزوير والتلاعب بالفيديو والتشكيك في صحة الأدلة المقدمة إلى المحكمة.

يشير الباحث لضرورة دمج الجهود المشتركة بين مُبرمجي تقنيات الذكاء الاصطناعي ذات الصلة بتحقيق العدالة الجنائية من جهة وبين العاملين في مجال القانون وأجهزة إنفاذه، كجمعيات القضاة، وكليات القانون، ونقابات المحامين من جهة أخرى، وذلك للمساهمة في إجراء بحوث التطبيقات المقترحة واختبارها لفهم إمكاناتها ونقاط ضعفها، لتكييفها مع الاحتياجات القضائية قبل طرحها على نطاق واسع.

يهيب الباحث بكليات القانون سرعة تدريب طلابها على "القانون الرقمي" واستخدامات تطبيقات الذكاء الاصطناعي ذات الصلة بالأُطُر القانونية.

يرجو الباحث توفير خبرة داخلية لدى أجهزة العدالة الجنائية يمكنها من تقييم تشغيل وتأثير تطبيقات الذكاء الاصطناعي وتقديم المشورة بشأنها للمستخدمين، ولها طلب تفسير كيفية عملها حين الحاجة دون الاحتجاج بحقوق الملكية الفكرية لمؤسسات الذكاء الاصطناعي وذلك لضمان اليقين القانوني.

قائمة المراجع

أولًا: المراجع العربية:

1. الأستاذ الدكتور/ أحمد عبد الظاهر – العدالة الجنائية الذكية "الكاميرات المحمولة على الجسم" - دراسة منشورة بمجلة القضاء والقانون – دائرة القضاء – السنة السابعة العدد 8 - أكتوبر 2020.
2. آلان بونيه - الذكاء الاصطناعي واقعه ومستقبله – ترجمة د/علي صبري فرغلي – سلسلة عالم المعرفة – الكويت – عدد أبريل 1993.
3. الجوانب القانونية للعقود الذكية والذكاء الاصطناعي – ورقة عمل مقدمة من تشيكيا إلى لجنة الأمم المتحدة للقانون التجاري الدولي – الدورة الحادية الخمسون – نيويورك 25 من يونيه – 13 يوليه 2018 – مطبوعات الجمعية العامة للأمم المتحدة – 960/A/CN.9.
4. الذكاء الاصطناعي – بلاي ويتباي – ترجمة دار الفاروق للاستثمارات الثقافية باتفاقية نشر مع مؤسسة محمد بن راشد آل مكتوم – طبعة 2008.
5. ديريك دوبريز - الاتحاد الأوروبي يناقش القضايا القانونية المتعلقة بالذكاء الاصطناعي – مقال مترجم من موقع ديجينوميكا - منشور بمجلة معهد دبي القضائي – العدد العد 10 - السنة السابعة - مارس 2019.
6. عميد دكتور/ غيث غانم سيف السويدي – مدير أكاديمية شرطة دبي – دور الذكاء الاصطناعي في تبسيط إجراءات التقاضي –دراسة قانونية تطبيقية على جريمة الشيك بدون رصيد "مقترح قضية الدقيقة الواحدة" – دراسة منشورة بمجلة القضاء والقانون – دائرة القضاء – السنة السابعة العدد 8 - أكتوبر 2020.
7. ميشيل باشيليت "مفوّضة الأمم المتّحدة السامية لحقوق الإنسان" - حقوق الإنسان في العصر الرقمي – متاح في 2021/01/06 على موقع: www.ohchr.org/AR/NewsEvents

ثانيًا: القوانين والقرارات:

8. دستور دولة الإمارات العربية المتحدة لسنة 1971.
9. قانون الإجراءات الجزائية الاتحادي الإماراتي رقم (35) لسنة 1992 وتعديلاته.
10. المرسوم بقانون اتحادي رقم 25 لسنة 2018صادر بتاريخ 23/09/2018م.الموافق فيه 13 محرم 1440هـ. بشأن المشروعات ذات الصفة المستقبلية الصادر بتاريخ 23 من سبتمبر 2018 والمنشور في عدد الجريدة الرسمية رقم 638 ملحق صفحة 9.
11. القانون الاتحادي رقم 10 لسنة 2019 بشأن تنظيم العلاقات القضائية بين السلطات القضائية الاتحادية والمحلية.
12. المرسوم بقانون اتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية الصادر في 20 من سبتمبر 2021 والمعمول به اعتبارًا من 02 من يناير 2022.
13. المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية الصادر في 20 من سبتمبر 2021 والمعمول به اعتبارًا من 02 يناير 2022.
14. قرار مجلس الوزراء رقم 14 لسنة 2019صادر بتاريخ 2018/09/23م.الموافق فيه 13 محرم 1440هـ. في شأن تنظيم إصدار التراخيص المؤقتة للمشاريع المبتكرة ذات الصفة المستقبلية الصادر بتاريخ 29 يناير 2019، والمنشور في عدد الجريدة الرسمية رقم 647 صفحة 739.
15. قرار حاكم دبي رقم 14 لسنة 2020 بشأن استخدام الكاميرات الأمنية في توثيق مهام منتسبي الشرطة – الصادر في 13 من أغسطس 2020، ونشر في الجريدة الرسمية لحكومة دبي السنة 54 العدد 483 بتاريخ 19 أغسطس 2020م.

ثالثًا: المراجع الأجنبية:

16. Algorithms in the Criminal Justice System: Risk Assessment Tools - Available online on 29/12/2020 at: https://epic.org/algorithmic-transparency/crim-justice/
17. Cambridge University – Helping police make custody decisions using artificial intelligence –Available online on 29/12/2020 at: https://www.cam.ac.uk/research/features/helping-police-make-custody-decisions-using-artificial-intelligence.
18. Camille Guillard - La justice prédictive et l'IA dans le procès pénal : risques et opportunités - consulté le 15/12/2020 https://www.justicepenale.net/post/la-justice-prédictive-et-l-ia-dans-le-procès-pénal-risques-et-opportunités.
19. Charte éthique européenne d'utilisation de l'intelligence artificielle dans les systèmes judiciaires (coe.int) - COMMISSION EUROPEENNE POUR L'EFFICACITE DE LA JUSTICE (CEPEJ) - Adoptée lors de la 31e réunion plénière de la CEPEJ (Strasbourg, 3-4 décembre 2018 - Conseil de l'Europe.
20. Christopher Rigano, "Using Artificial Intelligence to Address Criminal Justice

Needs" NIJ Journal 280, January 2019, https:// www.nij.gov/journals/280/ Pages.

21. Council of EUROPE - Parliamentary Assembly - Justice par algorithme – le rôle de l'intelligence artificielle dans les systèmes de police et de justice pénale - consulté le 15/12/2020 https://pace.coe.int/fr/files/25062#trace-1.
22. Facial recognition tech can help trace missing children despite privacy handicap – Available on line 12/01/2021 at: https://www.indialegallive.com/column-news/artificial-intelligence-face-recognition-raise-niti-aayog/
23. Interpol & Unicri (United Nations Interregional Crime and Justice Research Institute), Artificial Intelligence and Robotics for Law Enforcement, Available on Line on 10/01/2021 at: https://www.europarl.europa.eu/cmsdata/196207/UNICRI.
24. Laurence Pécaut-Rivolier et Stéphane Robin, consulté le 08/01/2021, Justice et intelligence artificielle, préparer demain : regards croisés d'une juriste et d'un mathématicien | Dalloz Actualité (dalloz-actualite.fr).
25. Les "juges virtuels" font leur apparition dans les tribunaux chinois - consulté le 05/01/2021 https://www.rtbf.be/info/monde/detail_la-technologie-de-l-intelligence-artificielle-fait-son-apparition-dans-les-tribunaux-chinois?id=10383210
26. Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, dite « Lemaire », JORF n°0235 -consulté le 30/12/2020 www.legifrance.gouv.fr/
27. Osonde A. Osoba & William Welser IV - The Risks of Artificial Intelligence to Security and the Future of Work - PE-237/1-RC (2017) – Available on line at www.rand.org.
28. PredPol is The Market Leader in Predictive Policing - Available online on 29/12/2020 at: https://www.predpol.com/about/
29. Wipo Magazine - BrightSign: a smart glove that gives a voice to those who cannot speak – Availabe on line on 06/01/2021 at BrightSign: a smart glove that gives a voice to those who cannot speak (wipo.int)

رؤيتنا

أن نكون مركزًا إقليميًا للتميز القانوني والعدلي

رسالتنا

تزويد أعضاء المجتمع القانوني بأفضل تدريب مهني
والتطوير المستمر وإكسابهم المعرفة الحديثة ذات الصلة

معهد دبي القضائي
DUBAI JUDICIAL INSTITUTE

P.O.Box.: 28552 Dubai
United Arab Emirates
Tel.: 00971 4 20 54 112
: 00971 4 20 54 110
Fax: 00971 4 28 27071
Web:www.dji.gov.ae
research@dji.gov.ae

www. / DubaiJudicial