القانون الدولي في مواجهة التحديات الرقمية

International Law in the Face of Digital Challenges

بحث مقدم من قبل
أ.م.د يسار عطيه اتويه
كلية القانون/ جامعة ميسان
yassar20210@gmail.com

الخلاصة :
يشهد العالم تطوراً سريعاً في التكنولوجيا الرقمية، مما يفرض تحديات جديدة على القانون الدولي، من حيث صياغة القواعد وتنفيذها في مواجهة المخاطر والفرص التي تطرحها البيئة الرقمية . فبتزايد الهجمات الإلكترونية أصبح من الضروري وضع إطار قانوني دولي يحدد المسؤوليات ويضمن التعاون بين الدول لمكافحة الجريمة السيبرانية وحماية البنية التحتية الرقمية. وضمان حقوق الأفراد في الخصوصية، خاصة مع انتشار تقنيات المراقبة ومعالجة البيانات عبر الحدود. لهذا تحتاج القوانين الدولية إلى معالجة قضايا أخلاقية وقانونية مرتبطة باستخدام الذكاء الاصطناعي في الحروب ، التجارة ، والرعاية الصحية، خاصة في ما يتعلق في حقوق الإنسان بالعالم الرقمي تلك الحقوق التي تشمل حرية التعبير، الوصول إلى الإنترنت ، وضمان عدم استخدام التكنولوجيا لقمع الحريات . كذلك هو الحال بالنسبة للتجارة الإلكترونية والملكية الفكرية التي تعرضت هي الأخرى للإضرار مع زيادة التجارة عبر الإنترنت ، فالقوانين الدولية تحتاج إلى التحديث لضمان حماية الملكية الفكرية وتنظيم المعاملات عبر الحدود. لذا تتطلب مواجهة هذه التحديات تعاوناً دولياً ، حيث يصبح القانون الدولي أداة أساسية في تحقيق التوازن بين الاستفادة من التطورات التكنولوجية وحماية الحقوق والمصالح الوطنية والدولية.
الكلمات المفتاحية : التكنولوجيا الرقمية ، التحديات الرقمية ، الملكية الفكرية ، المعاملات .

***Abstract*:**
The world is witnessing a rapid development in digital technology, which poses new challenges to international law in terms of formulating and implementing rules in the face of the risks and opportunities presented by the digital environment. With the increase in cyber attacks, it has become necessary to establish an international legal framework that defines responsibilities and ensures cooperation between countries to combat cybercrime and protect digital infrastructure. Rights to privacy, especially with the spread of surveillance technologies and data processing across borders. Therefore, international laws need to address ethical and legal issues related to the use of artificial intelligence in wars, trade, and healthcare. Especially with regard to human rights in the digital world, those rights include freedom of expression, access to the Internet, and ensuring that technology is not used to suppress freedoms. The same is the case for e-commerce and intellectual property,addressing these challenges requires international cooperation, as international law becomes an essential tool in achieving a balance between benefiting from technological developments and protecting national and international rights and interests.
Keywords: digital technology, digital challenges, intellectual property, transactions.

المقدمة

أولا/موضوع البحث :

إن التكنولوجيا الرقمية في العصر الحالي أصبحت جزءاً لا يتجزأ من الحياة اليومية ، حيث تزايد الاعتماد على الإنترنت والأنظمة الرقمية في مختلف المجالات الاقتصادية والاجتماعية والسياسية . هذا التحول الرقمي الكبير الذي تشهده البشرية يتيح إمكانيات غير محدودة في التواصل، والتجارة، والتعليم، ولكن في المقابل، يطرح تحديات قانونية وأخلاقية معقدة ، تتطلب استجابة من القانون الدولي الذي كان قد تأسس في ظل ظروف ومعطيات تختلف كثيراً عن تلك التي نعيشها اليوم . لقد أسهم الإنترنت في تحويل العالم إلى قرية كونية واحدة ، حيث أصبحت الحدود الجغرافية أقل تأثيراً على التفاعل بين الأفراد والمؤسسات والدول . ولكن هذا الانفتاح والتشابك الرقمي أدى أيضاً إلى ظهور تهديدات جديدة تتعلق بالأمن السيبراني، وخصوصية البيانات، وحقوق الإنسان الرقمية. بالإضافة إلى ذلك، أصبحت الجرائم الإلكترونية تتخذ أشكالاً متعددة ومعقدة، بدءاً من القرصنة على الشبكات الحكومية أو الشركات الكبرى وصولاً إلى التضليل الإعلامي عبر منصات التواصل الاجتماعي . ومن جانب آخر، يتطلب التفاعل الرقمي بين الدول في هذا الفضاء الافتراضي إنشاء قوانين ومعاهدات دولية تلزم الدول بأتباع قواعد مشتركة، لضمان حماية حقوق الأفراد والدول، والحفاظ على الأمن الرقمي والاقتصادي. لكن رغم الجهود المبذولة، لا يزال القانون الدولي يواجه صعوبات في مواكبة الابتكارات السريعة في هذا المجال ، ما يعكس الحاجة الملحة إلى تطوير قواعد قانونية مرنة وفعالة تلاؤم هذه التحديات المستمرة. إن القانون الدولي الذي نشأ لتنظيم العلاقات بين الدول في ميادين مختلفة، قد يجد نفسه في مأزق أمام هذه التطورات الرقمية المتسارعة التي تتجاوز الحدود التقليدية والتقسيمات الجغرافية. من هنا تنبع أهمية دراسة كيفية تفاعل هذا القانون مع المتغيرات الرقمية، وإمكانية إعادة صياغة آلياته بما يتوافق مع التطور التكنولوجي المتسارع. في هذا السياق، يسعى هذا البحث إلى تسليط الضوء على التحديات التي يواجهها القانون الدولي في مواجهة الثورة الرقمية، ويبحث في مدى فاعلية الأطر القانونية الحالية في معالجة قضايا مثل الأمن السيبراني، حماية البيانات، وحفظ حقوق الإنسان في العالم الرقمي. ومحاولة استكشاف كيف يمكن للدول والمنظمات الدولية التعاون فيما بينها لتطوير سياسات وقوانين مشتركة تضمن الاستفادة من الفضاء الرقمي بأمان وكفاءة، وتحدد إطاراً قانونياً يحفظ حقوق الأفراد ويمنع استغلال التكنولوجيا في الأعمال الإجرامية أو السياسية الضارة. بعد ان أصبح الإنترنت والفضاء الرقمي ساحة جديدة للتفاعل بين الدول والشركات والأفراد.

ثانياً/إشكالية البحث: يواجه القانون الدولي تحديات كبيرة في مواكبة التطورات الرقمية التي غيرت بشكل جذري الطريقة التي يتفاعل بها الأفراد والدول في الفضاء الافتراضي. على الرغم من وجود بعض المحاولات لتنظيم هذا الفضاء ، إلا أن معظم الأنظمة القانونية الحالية لا تزال تتسم بالبطء وعدم القدرة على التكيف مع سرعة الابتكارات التكنولوجية. في هذا السياق، تبرز العديد من الأسئلة التي تحتاج إلى إجابات شافية حول قدرة القانون الدولي على حماية الحقوق الرقمية وضمان الأمن السيبراني في ظل عالم مترابط تقنياً. فإلى أي مدى يمكن للقانون الدولي مواجهة التحديات التي تفرضها الثورة الرقمية. إن إشكالية البحث الأساسية تتلخص في التساؤل التالي:-

1- كيف يمكن للقانون الدولي مواجهة التحديات التي تفرضها الثورة الرقمية ، خاصة فيما يتعلق بحماية الحقوق الرقمية والأمن السيبراني، مع الحفاظ على المبادئ الأساسية التي يقوم عليها النظام القانوني الدولي؟وإلى أي مدى يمكن للقانون الدولي أن يواكب التحديات المتزايدة التي تطرأ في الفضاء الرقمي؟

2- كيف يؤثر تزايد التعقيد الرقمي على قدرة المعاهدات الدولية والقوانين المعمول بها في معالجة القضايا المتعلقة بالأمن السيبراني؟

3- هل توجد فجوات قانونية واضحة في تطبيق القانون الدولي على القضايا الرقمية مثل الجرائم الإلكترونية وحماية البيانات؟ وما هي العقبات التي يواجهها النظام القانوني الدولي في محاربة الجرائم الإلكترونية التي تتجاوز الحدود الجغرافية؟

4- كيف يمكن تنظيم حقوق الإنسان الرقمية ضمن إطار القانون الدولي؟ وهل تعترف الاتفاقيات والمعاهدات الدولية الحالية بحقوق الإنسان الرقمية، مثل الخصوصية وحماية البيانات الشخصية، وما هي التحديات المرتبطة بذلك؟

5- ما هو الدور الذي يمكن أن تلعبه المنظمات الدولية في وضع أطر قانونية مشتركة لمواجهة التحديات الرقمية؟ وكيف يمكن تعزيز التعاون الدولي لتطوير معايير مشتركة تنظم استخدام الإنترنت وحمايته من المخاطر الرقمية، مثل الهجمات السيبرانية؟ وكيف يمكن ضمان أن يكون القانون الدولي مرناً بما يكفي للتكيف مع الابتكارات التكنولوجية المستقبلية في الفضاء الرقمي؟

ثالثاً/أهمية البحث: إن الأهمية العلمية لهذا البحث مساهمته في إثراء النقاش الأكاديمي حول مدى فعالية القانون الدولي في التعامل مع القضايا الرقمية الناشئة. وما هو دور الرؤى والاستراتيجيات لصناع القرار في تطوير آليات قانونية لمواجهة الجرائم الإلكترونية وحماية الحقوق الرقمية. **وما** أهمية البحث القانونية في توضيح الفجوات القانونية التي يمكن أن تعيق مواجهة التحديات الرقمية على المستوى الدولي.

رابعاً/فرضية البحث: ينطلق البحث من الفرضية التالية ، يتمتع القانون الدولي بقدرة محدودة في مواجهة التحديات الرقمية الحالية بسبب تعقيد الظواهر الرقمية وسرعة تطورها، مما يستدعي تطوير قواعد قانونية جديدة وتعزيز التعاون الدولي لتحقيق فعالية أكبر في التعامل مع هذه التحديات.

خامساً/منهجية البحث:لتحليل الوضع الراهن للقانون الدولي ومدى استجابته للتحديات الرقمية تم استخدام المنهج الوصفي التحليلي . والمنهج المقارن لمقارنة تجارب دولية وإقليمية في تنظيم الفضاء الرقمي ومكافحة الجرائم السيبرانية. بالاضافة الى المنهج الاستقرائي لاستنتاج الحلول والاقتراحات بناءاً على تحليل الظواهر والقضايا المطروحة.

سادساً/نطاق البحث: في النطاق الموضوعي يتناول البحث القضايا القانونية المرتبطة بالتكنولوجيا الرقمية، مثل السيادة الرقمية، الجرائم الإلكترونية، حقوق الإنسان الرقمية، وحماية البيانات. وفي النطاق الزمني يركز البحث على الفترة من بداية القرن الحادي والعشرين وحتى الوقت الحالي، حيث تزايدت التحديات الرقمية بشكل ملحوظ. وأما في النطاق المكاني يشمل التحليل القانون الدولي بشقيه العام والخاص، مع التركيز على تطبيقات محددة على المستوى العالمي والإقليمي.

سابعاً/خطة البحث:-

المبحث الأول/ الإطار النظري للقانون الدولي والتحديات الرقمية.
المطلب الأول / مفهوم التحديات الرقمية.
الفرع الأول/ تعريف التحديات الرقمية في إطار القانون الدولي.
الفرع الثاني/ أهمية القانون الدولي في مواجهة التحديات الرقمية.
المطلب الثاني/ التطور القانوني الدولي في مواجهة التحديات الرقمية.
الفرع الأول/ الاتفاقيات الدولية في تطوير قوانين الأمن السيبراني .
الفرع الثاني/ دور الأمم المتحدة والمنظمات الدولية في تعزيز الأمن الرقمي.
المبحث الثاني/ التحديات المستقبلية وسبل التكييف القانوني.
المطلب الأول/ التحديات التقنية للأمن السيبراني والخصوصية في حماية البيانات الشخصية.
الفرع الأول/ التحديات الاجتماعية والاقتصادية للتجارة الإلكترونية ولحماية الملكية الفكرية .
الفرع الثاني/ تدابير الحماية للبيانات في مواجهة التحديات التقنية في إطار القوانين والتشريعات.
المطلب الأول/التحديات المستقبلية في المجالات الرقمية.
الفرع الأول/التقدم التكنولوجي وتأثيراته على السيادة الوطنية والعلاقات الدولية.
الفرع الثاني/ تعزيز التعاون بين الدول لتطوير آليات تنظيم عالمية.

المبحث الأول/ الإطار النظري للقانون الدولي والتحديات الرقمية

إن العلاقة بين القانون الدولي وتطور التقنيات الرقمية، تصدر من المواجهة بين النظام القانوني العالمي والتحديات الجديدة نتيجة للثورة الرقمية والتحول التكنولوجي السريع. فالقانون الدولي هو مجموعة القواعد والمبادئ التي تنظم العلاقات بين الدول والكيانات الدولية الأخرى، مثل المنظمات الدولية. إذ يستند الإطار النظري لهذا القانون إلى مبادئ السيادة، عدم التدخل، التعاون الدولي، واحترام حقوق الإنسان. ولكن مع ظهور التكنولوجيا الرقمية، بات القانون الدولي مطالباً بتوسيع مفاهيمه التقليدية لتشمل قضايا مثل الفضاء الإلكتروني (السيبراني)، وحقوق البيانات، وخصوصية الأفراد في السياق الدولي. لذا سنتناول في هذا المبحث مفهوم تلك التحديات الرقمية في إطار القانون الدولي والتطورات القانونية في مواجهة التحديات الرقمية. ودور الأمم المتحدة والمنظمات الدولية في تعزيز الأمن الرقمي.

المطلب الأول / مفهوم التحديات الرقمية

إن السيادة السيبرانية تعني التداخل بين حدود الدول في الفضاء الرقمي . الأمر الذي يثير تساؤلات حول كيفية فرض السيادة على الإنترنت.وما يتخللها من جرائم تتعلق بالنظام السيبراني تشمل الهجمات الإلكترونية، القرصنة، والاحتيال الرقمي، مما يتطلب إطاراً قانونياً دولياً مشتركاً لمكافحتها. الأمر الذي يفرض حماية للبيانات والخصوصية عن طريق صياغة القوانين الدولية لتتوافق مع التشريعات المحلية والدولية لحماية البيانات الشخصية. فالذكاء الاصطناعي وأخلاقياته هو الأخر يطرح أسئلة قانونية وأخلاقية تتعلق بالمسؤولية القانونية والشفافية. مما يحتاج القانون الدولي إلى آليات تحمي الإبداع الرقمي مع الحفاظ على حقوق الملكية الفكرية.

الفرع الأول/ تعريف التحديات الرقمية في إطار القانون الدولي

إن التحديات في اللغة تعني المصاعب أو المشكلات التي تتطلب مواجهة أو التغلب عليها. والتحدي في اللغة مأخوذ من (حدي) ويعني المجابهة والمواجهة، ويُستخدم للإشارة إلى العقبات أو المشكلات التي تحتاج إلى جهد للتغلب عليها[1]. ومنه يقال: "تحدى الأمر"، أي واجهه وصارع صعوباته. أما التحديات الرقمية مأخوذة من كلمة "رقم"، التي تعني العدد أو الإشارة العددية[2]. وفي العصر الحديث، أصبحت تُستخدم للإشارة إلى الأنظمة أو العمليات التي تعتمد على الأرقام الثنائية (0 و1)، وهي أساس التقنية الرقمية (Digital Technology). وهي نسبة إلى التقنيات الرقمية، وتشير إلى كل ما يتعلق بالأنظمة التي تعتمد على الحوسبة والبيانات الإلكترونية. وبالتالي، فإن "التحديات الرقمية" تعني المشكلات أو العقبات المتعلقة بالتقنيات أو الأنظمة الرقمية. ومن الناحية اللغوية، التحديات الرقمية تشير إلى المشكلات أو العقبات التي تبرز نتيجة التعامل مع الأنظمة أو الوسائل التقنية التي تعتمد على الحوسبة الرقمية والتكنولوجيا المتطورة. والتحديات الرقمية تجمع بين مفهوم المواجهة (التحدي) وبين البيئة الرقمية التي تمثل حقلاً واسعاً من الابتكار التقني والبيانات الإلكترونية ، مما يعكس صراعاً معقداً بين الإنسان والتكنولوجيا أو بين الكيانات المختلفة في ظل البيئة الرقمية . ويقال "فرضت

التكنولوجيا الرقمية تحديات جديدة تتعلق بخصوصية الأفراد ومراقبتهم عبر الإنترنت" [3].التحدي هنا يشير إلى العقبات التي تواجهها الدول والشركات في تحقيق التوازن بين استخدام التكنولوجيا وحماية خصوصية المستخدمين. ويقال التحدي في السيادة الرقمية يعني أصبحت سيطرة الدول الكبرى على البنية التحتية للإنترنت تحدياً رقمياً أمام الدول النامية. وهذا المثال يعكس استخدام كلمة "تحدي" للإشارة إلى الصراع بين الدول حول النفوذ في العالم الرقمي . أما عن التحدي الثقافي والمعرفي فيعدّ الانتقال إلى التعلم الرقمي تحدياً كبيراً في الدول التي تفتقر إلى البنية التحتية المناسبة. والتحدي في الجرائم الرقمية ، أي الهجمات السيبرانية تمثل تحدياً خطيراً للنظام الأمني العالمي.في كل مثال تم الإشارة إليه نلاحظ أن كلمة "تحديات" تحمل معنى المواجهة والصراع مع مصاعب ترتبط بالتطور التقني في مختلف المجالات (الأمن، الخصوصية، السيادة، الثقافة، وغيرها)، مما يعطي للتعبير "التحديات الرقمية" معنىً شاملًا في اللغة[4].

أما التعريف القانوني للتحديات الرقمية هي مجموعة الإشكاليات القانونية التي تنشأ نتيجة استخدام التكنولوجيا الرقمية والتطور التقني في شتى المجالات ، والتي تتطلب وضع قواعد وتشريعات جديدة أو تعديل القوانين القائمة لمواجهة تأثيراتها على الأفراد والدول[5]. تشمل هذه التحديات مسائل مثل الجرائم السيبرانية، حماية البيانات الشخصية، الملكية الفكرية الرقمية. فالتحديات الرقمية قانوناً هي مشكلات قانونية ناشئة عن التطورات التقنية، تفرض على الأنظمة القانونية الوطنية والدولية تحديث القواعد والتشريعات لتلبية متطلبات العصر الرقمي، مع ضمان تحقيق العدالة، حماية الحقوق، وصون الأمن السيبراني. فالتحديات الرقمية تشير إلى المسائل المستجدة الناتجة عن التطور التكنولوجي الرقمي والتي تتطلب اجتهاداً فقهيًا لتكييف الأحكام الشرعية بما يتوافق مع طبيعة هذه الظواهر الجديدة. وتشمل هذه التحديات القضايا الأخلاقية، الاجتماعية، والاقتصادية التي تثيرها التكنولوجيا الرقمية، مثل المعاملات المالية الإلكترونية. أما التحديات الرقمية في الفقه الإسلامي تُعد من القضايا المستجدة التي تتطلب اجتهاداً شرعياً يواكب تطورات العصر الرقمي[6]، مع الالتزام بمبادئ الشريعة ومقاصدها لتحقيق التوازن بين المصالح العامة والخاصة، ومواجهة المخاطر المحتملة بما يحقق العدالة والأمان في الفضاء الرقمي.

أما التعريف الاصطلاحي للتحديات الرقمية هو الإشارة إلى مجموعة من العقبات والمشكلات الناتجة عن استخدام التكنولوجيا الرقمية وتأثيرها على الأفراد، المؤسسات، والدول، وما يترتب على ذلك من أبعاد قانونية، اجتماعية، اقتصادية، وأمنية. تشمل هذه التحديات ظهور قضايا جديدة وغير مسبوقة تتطلب وضع أطر قانونية وتنظيمية لمعالجتها ، مع ضمان التوازن بين حقوق المستخدمين ومصالح الأطراف المختلفة.

وإن البُعد القانوني والتنظيمي للتحديات القانونية هو الحاجة إلى تطوير قواعد قانونية وطنية ودولية تُنظّم الأنشطة الرقمية ، مثل حماية البيانات والسيادة السيبرانية. والتغير المستمر في الطبيعة الديناميكية للتكنولوجيا الرقمية التي تجعل هذه التحديات تتطور بأستمرار، ما يتطلب استجابة مرنة ودائمة. وتعرف على أنها مظاهر جديدة للمشكلات التقليدية في عصر العولمة الرقمية ، إذ تتطلب جهوداً دولية ومحلية لخلق أطر تنظيمية وابتكار حلول قادرة على مواجهة هذه الظواهر، بما يحافظ على حقوق الأفراد وسيادة الدول، ويُعزّز الأمن والاستقرار العالمي[7]. والتحديات الرقمية في إطار القانون الدولي تشير إلى القضايا والمشكلات القانونية التي تنشأ نتيجة التطور السريع في التكنولوجيا الرقمية، وتأثيرها على العلاقات الدولية وحقوق الدول والأفراد. إذ تشمل الجرائم الإلكترونية تلك التي تُرتكب باستخدام الوسائل الرقمية، مثل القرصنة، الاحتيال عبر الإنترنت، والهجمات السيبرانية. وما يحدث من نزاعات حول الحق في الخصوصية مقابل استخدام البيانات الشخصية للأفراد عبر الحدود. في هذا السياق، تعكس التحديات الرقمية العلاقة بين القانون الدولي التقليدي (مثل قوانين السيادة وحقوق الإنسان) والمتطلبات الجديدة التي تفرضها العولمة الرقمية. تهدف هذه العلاقة إلى إيجاد توازن بين مصالح الدول، الشركات، والأفراد في العالم الرقمي، مع احترام المبادئ الأساسية للقانون الدولي. ويعرف النزاع المسلح السيبراني، بأنه استخدام الوسائل الالكترونية لغرض التأثير في مواقع الكترونية أخرى أو تدميرها أو الإضرار بها، أو استخدام الوسائل الالكترونية لتنفيذ هجمات عن بُعد ضد مواقع عسكرية أو مدنية سواء عن طريق الانترنت أو البرامج الالكترونية أو الرجال الآليين أو أي وسيلة الكترونية أخرى قد يصل اليها العلم فيما بعد[8]. وتعرف بأنها أي فعل يستخدم عن طريق شبكات الكترونية بهدف السيطرة أو التعطيل لبرامج الكترونية أخرى، وقد عرفت ايضاً بأنها (هجوم عبر الفضاء الالكتروني يهدف الى السيطرة على مواقع الكترونية أو بُنى محمية الكترونياً لتعطيلها أو تدميرها أو الإضرار بها)[9]وتعريف الحرب الإلكترونية "Electronic Warfare" بأنها مجموعة الإجراءات الإلكترونية المتضمنة استخدام بعض النظم والوسائل الإلكترونية الصديقة في استطلاع الإشعاع الكهرومغناطيسي الصادر من نظم العدو ووسائله ومعداته الإلكترونية المختلفة مع الاستخدام المتعمد للطاقة الكهرومغناطيسية في التأثير على هذه النظم والوسائل لمنع العدو، أو حرمانه، أو تقليل استغلاله للمجال الكهرومغناطيسي، فضلاً عن حماية الموجات الكهرومغناطيسية الصادرة من النظم والوسائل الإلكترونية الصديقة من استطلاع العدو لها، أو التأثير عليها[10]. ويمكن تعريفها على انها مجموعة الإجراءات التي تنفذ بهدف الاستطلاع الإلكتروني للنظم والوسائل الإلكترونية المعادية، والعمل على إعاقة هذه النظم والوسائل الإلكترونية ، ومقاومة الاستطلاع الإلكتروني المعادي ، وتحقيق استقرار عمل النظم الإلكترونية الصديقة تحت ظروف استخدام العدو أعمال الاستطلاع، والإعاقة الإلكترونية.

الفرع الثاني/ أهمية القانون الدولي في مواجهة التحديات الرقمية

إن القانون الدولي أداة لا غنى عنها لضمان الاستخدام الآمن والمسؤول للتكنولوجيا في العالم الرقمي . من خلال وضع القواعد والمعايير الدولية وتعزيز التعاون الدولي، الذي يساهم في مواجهة التحديات الرقمية بشكل شامل ومستدام . ومع استمرار التطور التكنولوجي يصبح تحديث وتطوير القانون الدولي ضرورة حتمية لتحقيق التوازن بين الابتكار وحماية الحقوق والمصالح المشتركة. فالقانون الدولي يواجه اليوم تحديات كبيرة في العصر الرقمي، حيث تلعب قواعده دوراً حيوياً في معالجة القضايا الناشئة. فهو يساهم في إنشاء إطار قانوني شامل لتنظيم الفضاء الرقمي بما يضمن التعاون بين الدول لمكافحة الجرائم الإلكترونية وحماية البنية التحتية الحساسة. مما يساعد في وضع معايير لحماية الخصوصية وحقوق الإنسان من التجسس والانتهاكات الرقمية، إلى جانب تعزيز الأمن السيبراني لمواجهة الحروب الإلكترونية والهجمات العابرة للحدود. يدعم التجارة الرقمية من خلال وضع قواعد لحماية حقوق المستهلكين وتنظيم العملات الرقمية ، بالإضافة إلى حماية الملكية الفكرية من القرصنة والنسخ غير القانوني. ويعزز التعاون الدولي في مواجهة التطورات التكنولوجية مثل الذكاء الاصطناعي وإنترنت الأشياء، ويعمل على تطوير آليات لضمان الاستخدام الآمن والمسؤول للتكنولوجيا[11]. كما يسعى القانون الدولي إلى تحقيق العدالة الرقمية بين الدول وضمان الوصول العادل إلى التكنولوجيا والبنية التحتية، مع تشجيع التوازن بين حرية التعبير وحماية البيانات . يتيح المجال لأبتكار حلول مستدامة للتحديات الرقمية مع مراعاة حقوق الأفراد والسيادة الوطنية. وقد يلعب القانون الدولي دوراً محورياً في تنظيم العلاقات الرقمية العابرة للحدود ، حيث يضع الأسس اللازمة للتعامل مع التحديات التي تنشأ عن التطور التكنولوجي السريع. يهدف إلى مكافحة الإرهاب الإلكتروني والجريمة المنظمة عبر الإنترنت من خلال تعزيز التعاون الأمني بين الدول، وإنشاء منصات لتبادل المعلومات بشكل سريع وفعال . وهذا يساعد في تنظيم استخدام الذكاء الاصطناعي والتكنولوجيا الناشئة لضمان الامتثال لمبادئ الأخلاقيات العالمية، والحد من تأثيراتها السلبية على المجتمعات. كما يضع إطاراً واضحاً للتعامل مع انتهاكات الأمن السيبراني التي تستهدف القطاعات الحيوية كالصحة والطاقة، ويعزز تطوير قواعد تمنع الدول من شن هجمات سيبرانية عدائية. في مجال التجارة الرقمية، إذ يسهم القانون الدولي في إزالة العوائق بين الأسواق، وضمان الشفافية في التعاملات الإلكترونية، ما يدعم الابتكار والنمو الاقتصادي العالمي. كما يدعم تنظيم المحتوى الرقمي ومكافحة الأخبار الزائفة وخطاب الكراهية على الإنترنت، مما يعزز بيئة رقمية أكثر أمانًا وعدالة. ويسعى لضمان حقوق الأفراد الرقمية كحرية الوصول إلى الإنترنت، مع حمايتهم من الاستغلال التجاري للبيانات الشخصية. بالإضافة إلى ذلك، يضع اتفاقيات تحدد مسؤوليات الشركات التقنية الكبرى تجاه المجتمعات، ويضمن توازناً بين المصالح الاقتصادية والاعتبارات الأخلاقية. فالقانون الدولي أصبح أداة حيوية لمواجهة التحديات الرقمية التي تتزايد مع تطور التكنولوجيا وانتشار الإنترنت. يلعب القانون الدولي دوراً محورياً في توفير الإطار القانوني والتنظيمي لضمان الأمن، العدالة، وحماية الحقوق في الفضاء الرقمي. فالتقنيات الرقمية تتجاوز الحدود الوطنية ، مما يجعل القانون الدولي ينسق بين الدول لتنظيم الأنشطة الرقمية. القانون الدولي ويساعد في وضع قواعد للتعامل مع القضايا العابرة للحدود مثل الجرائم الإلكترونية والاختراقات.

لقد غيرت المعلوماتية الالكترونية من طبيعة النزاعات والحروب، وأدخلت أساليب جديدة ومختلفة ومفاهيم بحاجة الى تقييم وصياغة، وحروب موجهة واخرى عبر الشبكة المعلوماتية. من هنا بدأ اهتمام المجتمع الدولي بالهجمات السيبرانية ففي عام1990 عَقدت الكلية البحرية الحربية الملكية أول مؤتمر قانوني بهذا الخصوص ثم ازداد الاهتمام الدولي بها بعد الهجمات الالكترونية ضد أستونيا في 2007/4/27 والتي استمرت لأسابيع، وقد تُوجهت الجهود الدولية المتعلقة بتنظيم النزاع المسلح السيبراني ، بإصدار" دليل تالين " حول القانون الدولي المطبق عليها، في عام2012 الذي بدأ العمل على صياغته منذ عام2009، وتم إكمال الجزء الثاني منه عام 2016[12]، وهو من إعداد اللجنة الدولية للخبراء وبدعوة من مركز التميز للدفاع السيبراني التعاوني التابع لحلف شمال الأطلسي ، وينطبق هذا الدليل على النزاع المسلح الدولي والداخلي ، وهو وثيقة غير ملزمة أعدها مجموعة من الخبراء، لكننا نأمل أن يحظى مستقبلاً بعنصر الإلزام كالمعاهدات الشارعة ويكون بمنزلة اتفاقيات جنيف الأربع لعام1949 والتي تتمتع بعنصر الالزام للكافة. ويمكن أن تكون الهجمة الالكترونية عشوائيةً أو مستهدف حسب النوايا الإجرامية والهدف منها. والتي تضرّ بالحاسوب وتعطله أو تسرق البيانات أو تستخدم أحد الحواسيب المخترَقة كنقطة انطلاقٍ لهجماتٍ أخرى. وتتبع وسائل مختلفة للتنفيذ منها البرمجيات الخبيثة malwareوالتصيد الاحتيالي phishing والفدية ransomware وتعطيل الخدمة denial of service وغيرها[13]. وهي قد تكون اعتداءاتٌ ذات أهدافٍ اجتماعيةٍ أو سياسيةٍ يتم تنفيذها أصلًا عبر الإنترنت. وتستهدف منظمات الشركات العامة أو الوطنية من خلال نشر برامج خبيثةٍ (فيروسات) وحظر الدخول للويب والمواقع الوهمية وغيرها من وسائل سرقة المعلومات الشخصية أو المؤسساتية من الجهات التي توجه لها الهجمات، مسببةً أضراراً بعيدة المدى[14]. فقد تتسبب الهجمات السيبرانية التي نشهدها اليوم في تكلفة اقتصادية كبيرة، وإن كان الجزء الأعظم منها ليس في إطار نزاع مسلح، ولم يتسبب لحسن الحظ في أضرار جوهرية للناس . غير أن هجمات أكثر تعقيداً وقد نجحت في تعطيل إمدادات خدمات أساسية لسكان مدنيين. ويبدو أن قطاع الرعاية الصحية على وجه الخصوص أكثر عرضة للهجمات السيبرانية ويتأثر كثيراً بها. كما تأثرت قطاعات أخرى من البنية التحتية المدنية من بينها أنظمة الكهرباء والمياه والصرف الصحي. وتفيد التقارير أن هذه الهجمات تزداد تواتراً، وتتعاظم حدتها بسرعة أكبر من أي توقعات[15]. عندما نؤكد على انطباق القانون الدولي الإنساني، فإننا لا نشجّع عسكرة الفضاء السيبراني، ولا نضفي شرعية على الحرب السيبرانية. وأي لجوء من الدول إلى القوة – سواء سيبرانية أو حركية – يظل محكوماً بميثاق الأمم المتحدة، لا سيما حظر اللجوء إلى القوة. والقانون الدولي

الإنساني إنما يوفر شريحة إضافية من الحماية ضد آثار الأعمال العدائية. فبموجبه، على سبيل المثال، يجب على المتحاربين احترام وحماية المرافق الطبية والعاملين فيها في جميع الأوقات. وبالتالي فإن الهجمات السيبرانية ضد قطاع الرعاية الصحية أثناء النزاع المسلح تُمثّل في معظم الأحوال انتهاكاً للقانون الدولي الإنساني. وعلى النهج ذاته، يتمتع المدنيون والأعيان المدنية والأشياء التي لا غنى عنها لبقاء السكان المدنيين بحماية خاصة بموجب مبادئ القانون الدولي الإنساني الخاصة بالتمييز، والتناسب، والاحتياط. وبالتالي، تُكفَل حماية قوية للبنية التحتية المدنية الحيوية ضد آثار الهجمات السيبرانية في أثناء النزاعات المسلحة.

المطلب الثاني/ التطور القانوني الدولي في مواجهة التحديات الرقمية

لقد استجابة الأنظمة القانونية الدولية للتحولات التي فرضتها الثورة الرقمية. مع التطور السريع في مجالات التكنولوجيا والاتصالات والذكاء الاصطناعي، مما برزت تحديات جديدة مثل الجرائم السيبرانية، خصوصية البيانات، التجارة الإلكترونية، وتنظيم الذكاء الاصطناعي. ولهذا نسعى إلى تحليل جهود القانون الدولي في تطوير أطر قانونية وتنظيمية لمواجهة هذه القضايا، مثل الاتفاقيات الدولية والتشريعات الوطنية والتعاون بين الدول. كما نركز على التوازن بين حماية الحقوق الفردية وتعزيز الابتكار، مع مراعاة التباينات بين الأنظمة القانونية في الدول المختلفة.

الفرع الأول/ الاتفاقيات الدولية في تطوير قوانين الأمن السيبراني

تعد الاتفاقيات الدولية إحدى الأدوات الأساسية التي تساهم في تطوير قوانين الأمن السيبراني عالمياً، نظراً للطبيعة العابرة للحدود للفضاء السيبراني والتهديدات المرتبطة به. في ظل الاعتماد المتزايد على التكنولوجيا في الحياة اليومية والاقتصاد والبنية التحتية، أصبحت الحاجة ملحّة إلى تعاون دولي لتأمين الفضاء السيبراني. فمفهوم الأمن السيبراني يشير إلى حماية الأنظمة الرقمية، والشبكات، والبيانات من الهجمات السيبرانية أو الاختراقات غير المصرح بها. مما دعت الحاجة إلى إبرام الاتفاقيات الدولية في الأمن السيبراني ونظرًا للطبيعة العالمية للفضاء السيبراني، يمكن أن تنطلق الهجمات من دولة ما لتستهدف دولًا أخرى دون قيود جغرافية. الأمر الذي يتطلب وضع إطار قانوني عالمي لمكافحة الجريمة السيبرانية. من خلال تعزيز التعاون بين الدول لتبادل المعلومات والتصدي للهجمات. فقد جاءت اتفاقية بودابست التي تبناها مجلس أوروبا وانضمت إليها دول غير أوروبية مثل الولايات المتحدة . هدفها توحيد التشريعات المتعلقة بجرائم الكمبيوتر، و تسهيل التعاون الدولي في التحقيقات السيبرانية. وتوفير أدوات للتعامل مع التحديات القانونية المرتبطة بالأدلة الرقمية. هي أول معاهدة دولية تهدف إلى مكافحة الجرائم الإلكترونية عن طريق التنسيق بين الدول في التشريعات والممارسات الأمنية. تم توقيعها في 23 نوفمبر 2001 ودخلت حيز التنفيذ في 1 يوليو 2004. الاتفاقية صادرة عن مجلس أوروبا، ولكنها مفتوحة للدول خارج القارة، مما يجعلها إطاراً عالمياً لمعالجة التهديدات الإلكترونية. هدفت لمكافحة الجرائم الإلكترونية من خلال وضع معايير قانونية لملاحقة الجرائم المتعلقة بأنظمة الكمبيوتر والإنترنت، كالقرصنة، والفيروسات، والاحتيال الإلكتروني. والعمل على توحيد التشريعات الوطنية بمساعدة الدول على مواءمة قوانينها المحلية لضمان تعاون فعال بين السلطات القانونية الدولية. وتعزيز التعاون الدولي في توفير إطار عمل للتنسيق بين الدول لمكافحة الجرائم العابرة للحدود. وحماية خصوصية البيانات والأمن والتركيز على مكافحة الجريمة دون انتهاك الحقوق الأساسية للمستخدمين مثل الخصوصية. من خلال تمكين الأدلة الرقمية لتسهيل جمع الأدلة الإلكترونية والتحقيق فيها واستخدامها في المحاكم[16].

لقد انشأت الأتفاقية أساس قانوني مشترك فهي تقدم مجموعة موحدة من المبادئ التي تساعد الدول على تطوير تشريعاتها الوطنية المتعلقة بالجرائم الإلكترونية. فالدول الموقعة تلتزم بتقديم المساعدة القانونية المتبادلة في التحقيقات المرتبطة بالجرائم الإلكترونية. فقد عملت الاتفاقية تسهل تبادل المعلومات حول الجرائم الإلكترونية بين الدول. وإيجاد آليات للتحقيق مع الأدلة الرقمية، بما في ذلك الوصول العابر للحدود والاحتفاظ بالبيانات.لقد حققت الأتفاقية انضمام واسع بأكثر من 60 دولة وقعت أو صادقت على الاتفاقية، بما في ذلك دول من خارج أوروبا مثل الولايات المتحدة وكندا. وساعدت الاتفاقية العديد من الدول في تطوير قوانين تتماشى مع متطلبات العصر الرقمي. إذ أصبحت الدول الموقعة تعمل بشكل أكثر تنسيقاً في التحقيقات وملاحقة الجرائم الإلكترونية العابرة للحدود . التعامل مع قضايا معقدة مثل الهجمات السيبرانية على البنية التحتية الحساسة، وتجارة البشر عبر الإنترنت، والاحتيال المالي. ومع هذه الانجازات التي حققتها الأتفاقية إلا إنها واجهت انتقادات منها. عدم تحقيق الانضمام العالمي للعديد من الدول الكبرى مثل روسيا والصين مما يحد من فعاليتها. وفيما يتعلق بالقضايا الخصوصية هناك مخاوف بشأن إمكانية إساءة استخدام الأدوات القانونية لجمع البيانات الرقمية. وكذلك هنالك ضعف في التعاون عبر الحدود الذي يتطلب استجابة سريعة، وهو أمر قد يكون معقداً في بعض الأحيان[17]. ومع ذلك إن اتفاقية بودابست تمثل خطوة حيوية في مواجهة التهديدات الإلكترونية العالمية. بفضل إطارها القانوني الموحد، فقد ساعدت في تحسين التعاون بين الدول وتقوية أنظمة الأمن السيبراني . ومع ذلك، لا تزال التحديات قائمة بسبب الحاجة إلى انضمام دول كبرى وبناء توازن بين مكافحة الجريمة وحماية الحقوق الفردية.أما اتفاقية شانغهاي للتعاون (SCO) فقد ركزت على مكافحة الإرهاب السيبراني والجريمة المنظمة عبر الإنترنت. وتعزيز التعاون الأمني بين الدول الأعضاء. تُركز بشكل كبير على الأمن القومي، وقد تتعارض مع مبادئ حرية الإنترنت وحقوق الإنسان . وأما اتفاقية مالابو للأمن السيبراني وحماية البيانات الشخصية (2014) فقد وضعت من قبل الاتحاد الإفريقي لمعالجة التحديات السيبرانية في القارة الإفريقية. وهدفها توفير إطار قانوني شامل لحماية الأنظمة الرقمية في إفريقيا . وتعزيز التعاون بين الدول الأعضاء في الاتحاد الإفريقي لمكافحة التهديدات السيبرانية. وضمان حماية البيانات الشخصية[18]. إن الاتفاقيات الدولية تمثل أداة حيوية لتطوير

قوانين الأمن السيبراني وضمان استقرار وأمان الفضاء السيبراني العالمي . ومع ذلك، فإن النجاح في هذا المجال يتطلب تعاوناً مستمراً، وتحقيق توازن بين الأمن واحترام الخصوصية وحقوق الإنسان. فالاتفاقيات الدولية في مجال الأمن السيبراني تعد حجر الأساس لحماية الفضاء الرقمي وضمان استقراره. ومع ذلك، فإن النجاح يعتمد على إرادة الدول للتعاون، ومواكبة التطورات التكنولوجية، وضمان توازن بين الأمن وحقوق الإنسان. تتطلب هذه الجهود تنسيقاً مستمراً بين الدول، المؤسسات الدولية، والقطاع الخاص لضمان تحقيق نظام رقمي آمن ومستدام.

الفرع الثاني/ دور الأمم المتحدة والمنظمات الدولية في تعزيز الأمن الرقمي

لقد لعبت الأمم المتحدة دوراً مهماً في تعزيز النقاش حول الأمن السيبراني من خلال منتديات مثل "مجموعة الخبراء الحكوميين" (GGE). والهدف هو وضع قواعد ومعايير سلوك الدول في الفضاء السيبراني، مع احترام سيادة الدول. فقد أنشأت الجمعية العامة للأمم المتحدة هذه المجموعة لتقديم توصيات حول كيفية استخدام تكنولوجيا المعلومات والاتصالات في إطار القانون الدولي. كذلك تسعى المجموعة إلى الحد من استخدام الفضاء السيبراني كأداة للعدوان وتحديد كيفية استجابة الدول للتهديدات الرقمية. فالأمم المتحدة تُعد إحدى المؤسسات الدولية الرائدة في مواجهة التحديات الرقمية والأمن السيبراني. مع التطور السريع للتكنولوجيا واعتماد المجتمعات عليها، برزت الحاجة الملحة إلى دور أممي لتنسيق الجهود الدولية وتنظيم الفضاء السيبراني. ينعكس دور الأمم المتحدة في تعزيز الأمن الرقمي عبر عدة محاور رئيسية، تشمل وضع الأطر القانونية، تعزيز التعاون الدولي، بناء القدرات، ودعم حوكمة الإنترنت. وعملها على صياغة معايير عالمية تتعلق بسلوك الدول في الفضاء السيبراني لضمان بيئة رقمية مستقرة وآمنة. فمجموعة الخبراء الحكوميين (UN GGE) والتصدي للجريمة السيبرانية وتشجع الدول الأعضاء على اعتماد التشريعات الوطنية التي تتماشى مع معايير الأمم المتحدة. ووضع منصات الحوار الدولي كالمنتدى العالمي لحوكمة الإنترنت (IGF) الذي يُعد منصة رئيسية تنظمها الأمم المتحدة منذ عام 2006 لمناقشة قضايا حوكمة الإنترنت والأمن الرقمي[19]. الذي يجمع بين الحكومات والقطاع الخاص والمجتمع المدني لتبادل الأفكار والحلول حول القضايا السيبرانية. وتعزيز الثقة بين الدول عبر تبادل المعلومات حول التهديدات الرقمية. وكذلك منتدى التعاون الاقتصادي لدول آسيا والمحيط الهادئ (APEC)، الذي يركز على تعزيز الأمن السيبراني في التجارة الإلكترونية[20] . وقد تعمل الأمم المتحدة مع منظمات إقليمية مثل الاتحاد الأوروبي والاتحاد الإفريقي لتعزيز القدرات الأمنية الرقمية في المناطق ذات الاحتياجات الخاصة. عبر وكالاتها المتخصصة، مثل الاتحاد الدولي للاتصالات (ITU)، تقدم الأمم المتحدة برامج تدريبية للدول الأعضاء لتحسين قدراتها في مجال الأمن السيبراني. وتساعد البرامج الدول النامية في تطوير بنية تحتية قوية وآمنة. وتعزيز الوعي العام من خلال مبادرات مثل الأسبوع العالمي للأمن السيبراني، دعمها حملات توعية للتعريف بأهمية الأمن الرقمي ودور الأفراد في تعزيز الحماية الإلكترونية. وتضع سياسات تضمن حماية الأنشطة الاقتصادية الرقمية، بما في ذلك التجارة الإلكترونية. من خلال العمل على إنشاء فرق دولية للاستجابة السريعة لحالات الطوارئ السيبرانية[21]. فالأمم المتحدة تسعى لحماية الحقوق الرقمية للأفراد، مثل الخصوصية وحرية التعبير، في مواجهة المراقبة غير القانونية والهجمات الإلكترونية. وتُشجع الحكومات على احترام المعايير الدولية عند تطوير سياساتها للأمن السيبراني.

أما المنظمات الإقليمية والدولية مثل حلف الناتو (NATO) الذي يركز على الأمن السيبراني ضمن استراتيجياته الدفاعية معينة لمعالجة قضايا معينة تهدد الأمن العالمي في مجالات مختلفة[22]. وما أطلقه الاتحاد الأوروبي من مبادرات في هذا المجال مثل "وكالة الأمن السيبراني الأوروبية" (ENISA) لتنسيق الجهود بين دول الاتحاد. وقد ضع لوائح مثل اللائحة العامة لحماية البيانات (GDPR) لتعزيز أمن البيانات[23]. أما منظمة التعاون الاقتصادي والتنمية (OECD) تقدم توجيهات للسياسات الرقمية الآمنة. من خلال دعم التعاون بين القطاعين العام والخاص[24]. فالمنظمات الدولية تعمل على بناء شراكات بين الحكومات والشركات الخاصة لتحسين أدوات الدفاع السيبراني. فمبادرات المنتدى الاقتصادي العالمي (WEF) تدعم تطوير حلول مبتكرة للأمن السيبراني. وكذلك مكافحة الجرائم السيبرانية من خلال تعاونها مع الإنتربول ومنظمات تنفيذ القانون، تسهم هذه الهيئات في تتبع الجرائم السيبرانية العابرة للحدود وتقديم مرتكبيها للعدالة[25]. فالاتحاد الإفريقي أعتمد اتفاقية مالابو (2014) لتعزيز الأمن السيبراني في القارة الإفريقية. وفي إطار مجموعة العشرين (G20) للأمن السيبراني الذي يناقش الأمن السيبراني كجزء من أجندة الاقتصاد الرقمي . ويدعو لتحسين أمن سلاسل التوريد الرقمية.وزيادة الاستثمار في بناء القدرات التقنية للدول النامية. وتعزيز الابتكار في حلول الأمن السيبراني[26]. أما عن دور القطاع الخاص والمنظمات غير الحكومية فكانت الشركات الكبرى مثل مايكروسوفت وجوجل تدعو إلى وضع اتفاقيات دولية جديدة لحماية الفضاء السيبراني، مثل مبادرة "اتفاقية جنيف الرقمية". أو إنشاء منظمات مثل الاتحاد الدولي للاتصالات (ITU) تعمل على تعزيز التعاون التقني وتقديم الدعم للدول في بناء قدراتها. وقد أصدرت الجمعية العامة للأمم المتحدة القرارين 63/55 و121/56 اللذين يضعان الإطار القانوني بشأن مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية، و إنشاء ثقافة أمنية عالمية للفضاء الحاسوبي. وقد اصدر مجلس الأمن القرار 2370في عام 2017 الذي يحث فيه الدول الأعضاء على العمل بصورة تعاونية لمنع الإرهابيين من حيازة الأسلحة، من خلال تكنولوجيات المعلومات والاتصالات، مع احترام حقوق الإنسان والحريات الأساسية والامتثال للالتزامات بموجب القانون الدولي[27].

إن التحديات التي تواجه الأمم المتحدة في هذا المجال هو انعدام الإجماع الدولي، والاختلافات السياسية بين الدول حول قضايا الأمن السيبراني تجعل من الصعب وضع قواعد ملزمة عالمياً. ولاسيما التطور السريع للتكنولوجيا الذي يجعل من

الصعب مواكبة المستجدات في مجال التهديدات السيبرانية. مع محدودية الموارد خصوصاً للدول النامية التي تحتاج إلى دعم إضافي لتطوير بنيتها التحتية الرقمية. ومع تلك التحديات تعمل الأمم المتحدة على خلق بيئة رقمية آمنة ومستقرة.

المبحث الثاني/ التحديات المستقبلية وسبل التكيف القانوني

إن المقصود في الأمن السيبراني هو عملية حماية الأنظمة والشبكات والبرمجيات من الهجمات الرقمية التي تهدف للوصول إلى المعلومات الحساسة أو تدميرها أو تعديلها أو تعطيل الأنظمة. مع التطور التكنولوجي السريع وزيادة الاعتماد على الإنترنت، أصبحت التحديات التي تواجه الأمن السيبراني أكثر تعقيداً وخطورة. وفيما يلي شرح مفصل لأبرز التحديات في هذا المجال لنتناول في مطلبين التحديات التقنية للأمن السيبراني والخصوصية في حماية البيانات الشخصية . والتحديات الاجتماعية والاقتصادية للتجارة الإلكترونية ولحماية الملكية الفكرية.

المطلب الأول/ التحديات التقنية للأمن السيبراني والخصوصية في حماية البيانات الشخصية

إن تطور التهديدات السيبرانية من خلال استخدام تقنيات متقدمة للهجمات يستخدمها مهاجمون بأستخدام أدوات متطورة مثل الذكاء الاصطناعي والتعلم الآلي لتنفيذ هجمات معقدة مثل التصيد الاحتيالي، وهجمات البرامج الضارة (Malware)، وبرامج الفدية (Ransomware). كهجمات يوم الصفر (Zero-Day Attacks) تلك الهجمات التي تستغل ثغرات غير معروفة في البرمجيات ، مما يجعل اكتشافها وإيقافها صعباً للغاية. والهجمات المستهدفة التي يقوم المهاجمون بتخصيص هجماتهم لاستهداف أفراد أو شركات بعينها، مما يزيد من خطورة وتأثير هذه الهجمات[28]. ولوجود نقص في الكفاءات البشرية في مجال الأمن السيبراني وزيادة الطلب على خبراء الأمن السيبراني على الرغم من النقص الحاصل في الكفاءات المؤهلة وعدم كفاية التدريب المستمر للموظفين في المؤسسات لتمكينهم من التعامل مع التهديدات الجديدة سبب حوادث كثيرة في عدم القدرة في السيطرة عليها. وهذا مما امتد أثره الى جوانب إجتماعية واقتصادية وشخصية سوف يتم الإشارة إليها لاحقاً.

الفرع الأول/ التحديات الاجتماعية والاقتصادية للتجارة الإلكترونية ولحماية الملكية الفكرية

إن التجارة الإلكترونية تعتبر من أبرز التطورات الاقتصادية والتكنولوجية التي شهدها العالم في العقود الأخيرة، لكنها تواجه العديد من التحديات الاجتماعية والاقتصادية، إضافة إلى قضايا حماية الملكية الفكرية التي تمثل جزءاً مهماً في تنظيم هذا القطاع. فالتجارة الإلكترونية تعتمد بشكل أساسي على الوصول إلى الإنترنت. هذه التقنية ليست متاحة بالتساوي في جميع المجتمعات، مما يؤدي إلى فجوة رقمية بين الطبقات الاجتماعية والمناطق الجغرافية المختلفة. فبعض المستخدمين يشكك في مصداقية المتاجر الإلكترونية، خصوصاً مع انتشار عمليات الاحتيال، مما يشكل عائقاً أمام تبني التجارة الإلكترونية على نطاق واسع. بالأظافة الى دخول التجارة الإلكترونية قد يؤثر على العادات الشرائية والثقافات المحلية، حيث قد تميل المجتمعات إلى تبني نمط استهلاكي عالمي، مما يهدد الصناعات المحلية الصغيرة. فالتجارة الإلكترونية قد تؤدي إلى تقليل فرص العمل في قطاعات التجزئة التقليدية، حيث تعتمد هذه المنصات بشكل أكبر على الأتمتة والتكنولوجيا. وقد تتفاوت عملة النمو بين الدول. فالدول المتقدمة تستفيد أكثر من التجارة الإلكترونية مقارنة بالدول النامية التي قد تواجه عقبات تتعلق بالبنية التحتية والتشريعات. وهناك جدل حول كيفية فرض الضرائب على التجارة الإلكترونية، خصوصاً عندما تكون الشركات تعمل عبر الحدود. هذا يؤدي إلى خسائر مالية للدول بسبب عدم وجود نظم ضريبية ملائمة. أما عن المنافسة غير العادلة فهنالك شركات كبرى مثل أمازون وعلي بابا تتمتع بموارد ضخمة تمكنها من التحكم بالسوق، مما يضع الشركات الصغيرة في وضع غير متكافئ[29]. فالتحديات المتعلقة بتوصيل المنتجات في الوقت المحدد وبتكلفة معقولة، خاصةً في المناطق الريفية أو الدول ذات البنية التحتية الضعيفة.

أما عن حماية الملكية الفكرية في التجارة الإلكترونية التي تعد من أهم القضايا المرتبطة بالتجارة الإلكترونية ، حيث تشمل حقوق النشر، والعلامات التجارية، وبراءات الاختراع. فالتحديات المتعلقة بالملكية الفكرية. كالمنتجات المقلدة تنتشر عبر الإنترنت منتجات مزيفة تنتهك حقوق الملكية الفكرية للمصنعين الأصليين . من خلال سرقة المحتوى الرقمي، مثل الكتب الإلكترونية، الموسيقى، والأفلام التي يتم تحميلها ومشاركتها بشكل غير قانوني. واستغلال العلامات التجارية يتم لجذب العملاء بطريقة غير قانونية. ومن هنا قد وضعت بعض الدول قوانين صارمة لمعالجة انتهاكات الملكية الفكرية في التجارة الإلكترونية، ولكن تنفيذها قد يواجه تحديات بسبب الطبيعة العابرة للحدود لهذه الأنشطة[30]. فالتجارة الإلكترونية تشكل فرصة هائلة للنمو الاقتصادي والاجتماعي، لكنها تتطلب معالجة التحديات المرتبطة بالعدالة الاجتماعية، والبنية التحتية، وحماية الملكية الفكرية. الحكومات والشركات مطالبة بتطوير سياسات وتشريعات تسهل هذا النوع من التجارة مع الحفاظ على حقوق الأفراد والمؤسسات. إن التجارة الإلكترونية، بسبب طبيعتها العابرة للحدود، تواجه صعوبات في الالتزام بالقوانين المحلية والدولية. خاصة مع وجود التشريعات المتفاوتة. فكل دولة لديها قوانينها الخاصة بالتجارة الإلكترونية، بما في ذلك الضرائب، حماية البيانات، وحقوق الملكية الفكرية. غياب التنسيق بين الدول يؤدي إلى صعوبات في التطبيق والتنفيذ. كذلك عملية مكافحة الجرائم الإلكترونية التي تعمل بشكل فاعل خاصة بعد تزايد الجرائم المرتبطة بالاحتيال، مثل سرقة بيانات العملاء، ما يتطلب تعزيز قوانين الأمن السيبراني. التي تعمل على تحديد المسؤول عن الانتهاكات في حالة المنتجات المقلدة أو المحتوى غير القانوني قد يكون معقدًا، خاصة مع وجود منصات وسيطة مثل أمازون وإيباي. فالعديد من المتاجر الإلكترونية تبيع منتجات بجودة أقل من المعلن عنها أو تقدم خدمات غير مطابقة

للوعود. فالمنصات الإلكترونية تُستخدم أحيانًا لتوزيع منتجات مزيفة أو منتهكة للملكية الفكرية، مما يضر الشركات الأصلية. اذ يمكن أن تؤدي هذه الممارسات إلى تقليل ثقة المستهلكين في التجارة الإلكترونية ككل[31].

رغم وجود قوانين صارمة في بعض الدول، فإن تتبع ومحاسبة المخالفين يظل معقداً، خاصة عندما يتم توزيع المحتوى عبر منصات غير رسمية[32]. وهذا يحدث خاصةً عندما تكون الملكية الفكرية غير محمية، أذ يتردد المبتكرون والمصممون في استثمار وقتهم ومواردهم في تطوير منتجات جديدة. بسبب أنتشار السلع المقلدة الذي يثبط الإبداع ويؤثر على جودة المنتجات في الأسواق. فالدول التي لا تطبق قوانين صارمة لحماية الملكية الفكرية تخسر مليارات الدولارات سنوياً بسبب تهريب المنتجات المزيفة. مما يضعف الاقتصاد المحلي، خاصة في الصناعات القائمة على الإبداع، مثل التكنولوجيا، والترفيه، والأزياء.

فتوحيد التشريعات الدولية من خلال التنسيق بين الدول لوضع قوانين موحدة تُسهل تنظيم التجارة الإلكترونية وحماية حقوق الملكية الفكرية عالميًا. وكذلك استخدام التكنولوجيا تقنية البلوك تشين أذ يمكن استخدامها لتسجيل وتتبع ملكية المنتجات الرقمية أو المادية، مما يقلل من احتمالية التزوير. ومن خلالها يمكنه اكتشاف المحتوى غير القانوني ومنع انتهاكات حقوق الملكية الفكرية على المنصات الإلكترونية. بالإضافة للقيام بحملات توعية تستهدف المستهلكين حول أهمية إحترام حقوق الملكية الفكرية، وكيفية التعرف على المنتجات المقلدة. نشر برامج تعليمية للبائعين حول التزاماتهم القانونية وأهمية الالتزام بمعايير الملكية الفكرية. لاسيما التعاون بين القطاعين العام والخاص ، فالشراكة بين الحكومات والشركات الكبرى لتطوير سياسات فعالة ومتكاملة لمكافحة القرصنة وانتهاك الملكية الفكرية. كذلك تطوير آليات حماية المستهلك، من خلال إنشاء منصات تسوية منازعات إلكترونية تُسهل على المستهلكين والبائعين حل الخلافات بشكل عادل وسريع. وتحسين سياسات الاسترجاع وضمان الشفافية في العروض التجارية. فالتجارة الإلكترونية تحمل إمكانات هائلة للنمو الاقتصادي والاجتماعي، لكنها تتطلب معالجة حاسمة للتحديات المرتبطة بحماية الملكية الفكرية وتحقيق العدالة الاجتماعية. يجب على الحكومات والشركات أن تستثمر في التكنولوجيا، التوعية، والتشريعات لضمان أن تكون هذه الصناعة مستدامة ومتوازنة في المستقبل.

الفرع الثاني/ تدابير الحماية للبيانات في مواجهة التحديات التقنية في إطار القوانين والتشريعات

إن تزايد استخدام أجهزة الإنترنت المتطورة أدى إلى زيادة الهجمات، حيث تكون هذه الأجهزة غالباً غير محمية بشكل كافٍ، فالثغرات الأمنية في الإنترنت تمثل بوابة سهلة للمهاجمين للوصول إلى الشبكات. فقد تأتي التهديدات من داخل المؤسسة نفسها، سواء بسبب الإهمال أو السلوك المتعمد من قبل الموظفين. وصعوبة اكتشاف هذا النوع من التهديدات تجعلها خطيرة للغاية. لذلك تحتاج المؤسسات إلى الامتثال لمجموعة متزايدة من القوانين واللوائح المتعلقة بحماية البيانات مثل اللائحة العامة لحماية البيانات (GDPR) أو قانون حماية البيانات الشخصية[33].

إن الكثير من المؤسسات والأفراد لا يدركون أهمية الأمن السيبراني، بسبب ضعف الوعي بالأمن السيبراني مما يجعلهم عرضة للهجمات. وعدم إتباع ممارسات أمان بسيطة، مثل استخدام كلمات مرور قوية أو تحديث البرمجيات، يزيد من احتمالية التعرض للاختراق. فقد يستهدف المهاجمون نقاط الضعف في سلاسل التوريد (الموردين أو الشركاء) للوصول إلى أنظمة الشركات. ويمكن أن تكون هذه الهجمات واسعة النطاق وتسبب أضراراً كبيرة. بالاضافة الى إن الاستثمار في الأدوات الحديثة والبرامج المتقدمة لحماية الأنظمة يكلف المؤسسات مبالغ كبيرة. قد تجد الشركات الصغيرة صعوبة في تخصيص ميزانية كافية لمواجهة هذه التحديات. ولكن بالإمكان التخفيف من هذه التكاليف بالعمل على التوعية والتدريب لرفع مستوى الوعي لدى الموظفين وتعليمهم كيفية اكتشاف التهديدات. وتطوير الأدوات الأمنية من خلال الاستثمار في أدوات الذكاء الاصطناعي وتكنولوجيا الكشف المبكر عن الهجمات. كذلك تحديث الأنظمة والبرمجيات بشكل دوري لسد الثغرات. والتعاون الدولي في تبادل المعلومات حول التهديدات بين الحكومات والمؤسسات. وتعزيز سياسات الأمن في وضع سياسات وإجراءات صارمة لحماية البيانات وتقليل المخاطر. فالأمن السيبراني هو معركة مستمرة تتطلب تكاملاً بين التقنية والوعي البشري لمواجهة التهديدات المتزايدة. وحماية الخصوصية والبيانات الشخصية تعد جزءاً أساسياً من الأمن السيبراني، خاصةً في ظل التطور التكنولوجي الهائل وزيادة الاعتماد على الإنترنت. مع ازدياد جمع البيانات الشخصية واستخدامها من قبل الشركات والمؤسسات، باتت الخصوصية تواجه تحديات جديدة تحتاج إلى معالجة دقيقة. إذ إن الجهود المؤسساتية تهدف لضمان أمان وسرية المعلومات الشخصية، ومنع استخدامها أو مشاركتها بشكل غير قانوني أو غير أخلاقي. أكيد بلا شك إن زيادة استخدام التطبيقات والمنصات الرقمية يؤدي إلى جمع كميات هائلة من البيانات عن الأفراد . وقد يتم جمع البيانات حتى دون علم المستخدمين أحياناً، مما يعرض الخصوصية للخطر[34]. ويحدث هذا بسبب تعرض البيانات للاختراق ووجود الثغرات الأمنية في الأنظمة أو البرمجيات. اذ يمكن أن تسفر عمليات القرصنة عن تسريب بيانات حساسة. وقد تستخدم بصورة غير قانونية للبيانات . كبيع البيانات الشخصية أو مشاركتها مع أطراف ثالثة دون موافقة المستخدم. وقد تستغل البيانات للإعلانات المستهدفة أو الاحتيال.مع غياب الشفافية لبعض الشركات التي لا توضح بشكل كافٍ كيفية جمع البيانات أو استخدامها. وعدم وجود سياسات خصوصية واضحة يجعل من الصعب على المستخدمين التحكم في بياناتهم. بالاضافة للتقنيات مثل الذكاء الاصطناعي والتعلم الآلي التي تكون قادرة على تحليل كميات ضخمة من البيانات الشخصية لأستنتاج معلومات أكثر دقة عن الأفراد. مما قد يستهدف الفرد أو الشركة لسرقة البيانات الشخصية واستخدامها في الابتزاز أو الاحتيال. إن الإطار القانوني لحماية البيانات الشخصية يتضح من خلال الإجراءات التي اتخذتها

العديد من الدول حيث وضعت قوانين وتشريعات لحماية البيانات الشخصية وضمان الخصوصية ، ومن أبرزها اللائحة العامة لحماية البيانات (GDPR) التي تطبق في الاتحاد الأوروبي . وتهدف إلى منح الأفراد سيطرة أكبر على بياناتهم الشخصية. أذ تشمل متطلبات مثل الموافقة الصريحة لجمع البيانات ، وحق الأفراد في طلب حذف بياناتهم. وكذلك قانون حماية خصوصية المستهلك في كاليفورنيا (CCPA) [35]الذي يمنح سكان كاليفورنيا حقوقاً مماثلة لحماية بياناتهم . ويشترط الكشف عن كيفية جمع البيانات واستخدامها. وهنالك البعض من الدول العربية التي أصدرت قوانين لحماية البيانات ، مثل قانون حماية البيانات الشخصية المصري وقانون حماية البيانات في السعودية. إن حماية الخصوصية ليست مجرد التزام قانوني، بل هي مسؤولية أخلاقية ومهنية تجاه الأفراد والمجتمع.

المطلب الأول/التحديات المستقبلية في المجالات الرقمية

إن التحديات المستقبلية في المجالات الرقمية تمثل قضايا متعددة تواجه الأفراد والمؤسسات والحكومات مع استمرار الثورة الرقمية وتطور التكنولوجيا. مع زيادة الاعتماد على الأنظمة الرقمية، تتزايد الهجمات الإلكترونية والاختراقات التي تهدد خصوصية الأفراد وسلامة المؤسسات. إذ تعتمد هذه التقنيات على تعزيز التجربة البشرية في مجالات التعليم، الطب، الترفيه، والعمل. فتطوير أجهزة أكثر كفاءة وأقل تكلفة للوصول إلى شريحة أوسع من المستخدمين. ومعالجة المخاوف المرتبطة بالعزلة الاجتماعية الناجمة عن الانغماس في العالم الافتراضي. وحماية البيانات الشخصية التي يتم جمعها من خلال هذه الأجهزة. تعزيز الثقة لدى الأفراد في المجالات الالكترونية والاقتصاد والتجارة الإلكترونية من خلال ممارسات سياسات شفافة. تحسين أنظمة الدفع الرقمي لضمان الأمان والسهولة. ومواجهة الجرائم الإلكترونية مثل الاحتيال المالي. فالتحديات المستقبلية في المجالات الرقمية تعكس الحاجة إلى توازن بين التطور التكنولوجي والحفاظ على القيم الإنسانية والبيئية. إذ يتطلب التصدي لهذه التحديات تعاوناً بين الحكومات، القطاع الخاص، والأفراد لضمان الاستفادة من هذه التطورات مع تقليل المخاطر المحتملة. ومع استمرار تقدم المجالات الرقمية، فإن مواجهة هذه التحديات تتطلب تكاتف الجهود بين جميع الأطراف المعنية. تبني استراتيجيات مبتكرة وشاملة، مع التركيز على القيم الأخلاقية والاستدامة، سيضمن مستقبلاً رقمياً آمناً وعادلاً للجميع.

الفرع الأول/التقدم التكنولوجي وتأثيراته على السيادة الوطنية والعلاقات الدولية

إن التقدم التكنولوجي يمثل أحد أهم محركات التغيير في القرن الحادي والعشرين، وهو يترك تأثيرات عميقة على السيادة الوطنية والعلاقات الدولية. فقد أصبحت البيانات مورداً استراتيجياً، ولكن العديد من الدول تواجه صعوبة في السيطرة على تدفق البيانات عبر الحدود. فأن فقدان السيادة على البيانات الوطنية بسبب سيطرة الشركات الكبرى متعددة الجنسيات. أدى إلى صعوبة التحكم في المعلومات التي تؤثر على الأمن الوطني أو الثقافي. ومع زيادة التهديدات السيبرانية، أصبحت الدول تواجه صعوبات في حماية بنيتها التحتية الرقمية من الهجمات الإلكترونية على المؤسسات الحكومية والشركات التي قد تعطل الاقتصاديات الوطنية. مما يتطلب ظهور حاجة لتطوير تقنيات محلية لحماية الشبكات الوطنية من التهديدات الأجنبية. لهذا أصبحت الدول تعتمد بشكل كبير على التكنولوجيا المتطورة في مجال الدفاعات العسكرية المتقدمة. لكن سباق التسلح التكنولوجي يعزز عدم الاستقرار بين الدول. وظهور تهديدات جديدة مثل الطائرات المسيّرة والروبوتات العسكرية التي تقوّض الحدود التقليدية للحرب. لذلك تعتبر الشركات التقنية الكبرى مثل "جوجل" و"ميتا" تمارس تأثيراً واسعاً على سياسات الدول[36]. فقد تتدخل الشركات في سياسات الدول من خلال التحكم في تدفق المعلومات وقدرتها للضغط على الحكومات لتحقيق مكاسب اقتصادية. لهذا السبب الدول تتنافس لتطوير تقنيات متقدمة مثل الذكاء الاصطناعي، الحوسبة الكمية، وتقنيات الفضاء لحماية سيادتها من التدخل.

لقد تصاعد التوترات بين القوى الكبرى مثل الولايات المتحدة والصين لتشكيل تحالفات تقنية بين الدول لتعزيز التعاون أو مواجهة التهديدات. فالهجوم الإلكتروني على خطوط الأنابيب الأمريكية (Colonial Pipeline) عطل البنية التحتية للطاقة وأظهر هشاشة الاقتصاديات أمام التهديدات السيبرانية[37]. فقد أصبحت الدول تستخدم التكنولوجيا لتعزيز نفوذها السياسي والاقتصادي. فظهور تحديات عالمية تحتاج إلى تعاون دولي مثل الأمن السيبراني، تنظيم الذكاء الاصطناعي، وحوكمة الإنترنت. والحاجة إلى وضع معايير دولية لتنظيم استخدام التكنولوجيا. وتصاعد النزاعات حول من يسيطر على البنية التحتية العالمية مثل الإنترنت والأقمار الصناعية. أدت إلى ظهور تأثير التكنولوجيا على التنمية الاقتصادية، فقد أخذت الدول التي تتأخر في تبني التكنولوجيا تواجه تحديات اقتصادية كبرى. فزيادة الفجوة بين الدول المتقدمة والنامية. تشكيل علاقات غير متكافئة حيث تعتمد الدول النامية على التقنيات المستوردة. فسباق الذكاء الاصطناعي بين القوى الكبرى أدى إلى استثمار الولايات المتحدة والصين في الذكاء الاصطناعي تؤثر على ميزان القوى العالمي. فقد استخدمت الولايات المتحدة ضغوطاً على حلفائها لمنع استخدام تقنيات هواوي، مما أثار جدلاً حول السيادة التقنية.

إن تعزيز السيادة التكنولوجية يحدث من خلال الاستثمار في البحث والتطوير لتعزيز قدرة الدول على إنتاج تقنيات محلية مع تقليل الاعتماد على الشركات التقنية الأجنبية. نعم تعزيز الشراكات بين الدول لمواجهة التحديات المشتركة مثل الجرائم السيبرانية.ووضع معايير دولية لتنظيم استخدام التكنولوجيا. وسنّ قوانين تضمن حماية الخصوصية دون التأثير على الأمن القومي. وتحسين إدارة البيانات لضمان عدم استغلالها من قبل أطراف أجنبية. يمثل فرصة كبيرة للدول لتعزيز مكانتها الاقتصادية والسياسية، لكنه يطرح تحديات كبيرة للسيادة الوطنية والعلاقات الدولية. تحتاج الدول إلى استراتيجيات متوازنة تجمع بين تعزيز الأمن والسيادة، والتعاون الدولي، مع ضمان الاستخدام الأخلاقي والمسؤول للتكنولوجيا. ففي

عصر اقتصاد البيانات، أصبحت الدول والمؤسسات تعتمد على جمع وتحليل كميات هائلة من البيانات لأتخاذ قرارات إستراتيجية. ومع ذلك، فإن التدفق الحر للبيانات عبر الحدود يؤدي إلى تهديد للسيادة الرقمية. فيمكن استخدام البيانات في عمليات التجسس الإلكتروني أو التأثير على الانتخابات أو نشر الفوضى ، كما حدث في قضية تدخل روسيا في الانتخابات الأمريكية عام 2016 عبر وسائل التواصل الاجتماعي. وكما حدث مع هجوم "Stuxnet" الذي استهدف المنشآت النووية الإيرانية عام 2010[38] . لقد أصبحت البنية التحتية الحيوية، مثل شبكات الطاقة، وأنظمة النقل، والأنظمة الصحية، تعتمد بشكل كبير على التكنولوجيا الرقمية ، مما يجعلها هدفاً للهجمات الإلكترونية. فالهجمات على المؤسسات الحكومية . لهذا يحتاج الأمن السيبراني إلى استثمارات ضخمة وتطوير مستمر للبنية التحتية الدفاعية لمواكبة تطور الهجمات. ففي برنامج سباق التسلح السيبراني نجد دول مثل الصين والولايات المتحدة أصبحت تستثمر بشكل كبير في تطوير أسلحة سيبرانية قادرة على إلحاق أضرار إستراتيجية بالدول المنافسة. والجميع يعلم إن التكنولوجيا غيرت طبيعة الحروب من القتال التقليدي إلى حروب تعتمد على التقنيات الذكية. فظهور الروبوتات العسكرية، واستخدام الطائرات بدون طيار والأسلحة ذاتية التحكم أثار جدلاً حول المسؤولية الأخلاقية والقانونية. فلم تعد الحدود الجغرافية كافية لحماية الدول من الهجمات الإلكترونية أو الأسلحة الذكية يمكن أن تنفذ عبر الإنترنت أو الأقمار الصناعية. كأستخدام الطائرات بدون طيار في النزاعات ، مثل الغارات الأمريكية بطائرات "درون" في الشرق الأوسط، يعكس كيف يمكن للتكنولوجيا تجاوز السيادة الوطنية بسهولة.

إن التكنولوجيا لم تؤثر فقط على الاقتصاد والأمن، بل طالت أيضاً الهوية الثقافية والسياسية للدول. فأستخدام وسائل التواصل الاجتماعي لنشر الأخبار الزائفة أو التأثير على الرأي العام كما حدث خلال الربيع العربي. وزيادة تأثير الثقافة الغربية عبر منصات البث الرقمي مثل نتفليكس[39]، يؤدي إلى تآكل الهوية الثقافية الوطنية. ففي الصين يتم تقييد الوصول إلى العديد من المنصات الغربية مثل "فيسبوك" و"تويتر" لحماية الثقافة الوطنية. وقد فرض الهند حظراً على تطبيق "تيك توك" الصيني لأسباب تتعلق بالخصوصية والأمن[40].

إن التنافس بين الولايات المتحدة والصين والدول العظمى في مجالات الذكاء الاصطناعي وشبكات الجيل الخامس (G5) يعكس تحول التكنولوجيا إلى سلاح استراتيجي. فالنزاع بين الولايات المتحدة وشركة هواوي، حيث فرضت واشنطن قيوداً على إستخدام تقنيات الشركة لأسباب أمنية. فالدول المتقدمة تروج لتقنياتها في الدول النامية لكسب نفوذ استراتيجي، كما تفعل الصين من خلال مبادرة "طريق الحرير الرقمي" من خلال إعتماد الاقتصاد العالمي على سلاسل التوريد الرقمية، مما يجعل الدول مترابطة بشكل غير مسبوق. فأزمات سلسلة التوريد كما حدث خلال جائحة كورونا، حيث أدت الإغلاقات إلى تعطيل شبكات التوريد العالمية[41]. وتأثير القرارات السياسية كالعقوبات الأمريكية على شركات التقنية الصينية أثرت على الاقتصاد العالمي ، خاصة في قطاعات أشباه الموصلات. لذا فأن استخدام تقنيات المراقبة والتجسس والتكنولوجيا العسكرية يثير أسئلة أخلاقية حول مسؤولية الدول . مع غياب إطار دولي في عدم وجود قوانين دولية واضحة تنظم استخدام الذكاء الاصطناعي في الحروب أو القرارات السياسية. مع توسع تأثير التكنولوجيا، أصبحت هناك حاجة ملحة لإطار عالمي لتنظيمها والحد من استخداماتها غير الأخلاقية .

الفرع الثاني/ تعزيز التعاون بين الدول لتطوير آليات تنظيم عالمية

مع تزايد تأثير التكنولوجيا على جميع جوانب الحياة، ظهرت الحاجة إلى آليات تنظيم عالمية فعّالة. كالذكاء الاصطناعي، الحوسبة الكمية، والبلوكشين، التي تتطلب نهجاً عالمياً لتجنب الفوضى التنظيمية ولضمان الاستخدام العادل والمسؤول لهذه التقنيات. فالطبيعة العابرة للحدود، فالتقدم التكنولوجي يتجاوز الحدود الجغرافية، مما يجعل من الصعب على دولة واحدة أن تضع قوانين وتنظيمات فعّالة. فبوجود الإنترنت إن الاقتصادات الرقمية تجعل من السهل نقل البيانات ورأس المال بين الدول، مما يخلق تحديات تنظيمية[42].

إن الأضرار الناتجة عن التكنولوجيا، مثل التضليل الإعلامي ، تغير المناخ الرقمي (البصمة الكربونية للتكنولوجيا)، والجرائم السيبرانية، تؤثر على جميع الدول بشكل متساوٍ . وان الحاجة إلى وضع معايير موحدة في ظل وجود اختلافات في القوانين بين الدول قد يؤدي إلى استغلال الثغرات القانونية. فالشركات الكبرى قد تختار العمل في دول ذات لوائح أقل صرامة ، مما يؤدي إلى سباق نحو القاع في التنظيم. ومن الأمثلة على المجالات التي تحتاج إلى تعاون دولي هي، تنظيم الذكاء الاصطناعي ،انحياز الخوارزميات،مخاوف من الاستخدام العسكري للذكاء الاصطناعي، التأثير على الوظائف والأسواق. فالحلول الممكنة لها تكمن في إنشاء منظمة دولية للذكاء الاصطناعي تشبه "الوكالة الدولية للطاقة الذرية" لمراقبة استخدامه. وكذلك تطوير مبادئ أخلاقية مشتركة لأستخدام الذكاء الاصطناعي. من خلال توقيع معاهدات دولية تحظر الهجمات السيبرانية على البنى التحتية المدنية. وكذلك إنشاء نظام عالمي لمشاركة المعلومات حول الهجمات الإلكترونية. وتعزيز دور منتدى حوكمة الإنترنت (IGF) تحت رعاية الأمم المتحدة[43]. ووضع قوانين عالمية تضمن توازناً بين حرية التعبير وأمن الدول. وتنظيم العملات الرقمية وتقنية البلوكشين.في الحد من غسيل الأموال وتمويل الإرهاب. والتقلبات الأسواق المالية الناتجة عن العملات الرقمية. في إنشاء أطر تنظيمية موحدة بين البنوك المركزية. وتطوير قوانين مشتركة لتداول العملات الرقمية.

إن المعاهدات الدولية تلعب دوراً اساسياً في الحد من انتشار الجرائم السبرانية. فاتفاقية باريس للمناخ، أتاحت للدول التوصل إلى معاهدات ملزمة بشأن استخدام التكنولوجيا والتنظيم. والعمل على إنشاء منظمات متخصصة لتنظيم مجالات

معينة مثل الذكاء الاصطناعي والعملات الرقمية يمكن أن تضم ممثلين من الحكومات، القطاع الخاص، والمجتمع المدني. كذلك تشكيل تحالفات إقليمية (مثل الاتحاد الأوروبي) لقيادة جهود تنظيمية على المستوى العالمي. وتوسيع دور منتديات مثل "منتدى الاقتصاد العالمي" (WEF) و"مجموعة العشرين" (G20) لتشمل النقاشات حول التنظيم التكنولوجي[44].

إن التحديات أمام التعاون الدولي تنشأ نتيجة اختلاف المصالح الوطنية فالدول الكبرى مثل الولايات المتحدة والصين لديها سياسات مختلفة بشأن التكنولوجيا، مما قد يعرقل التوصل إلى توافق بسبب نقص الثقة بين الدول. ومن جانب آخر زيادة التوترات الجيوسياسية قد تجعل الدول تتردد في مشاركة المعلومات أو العمل معاً. أما الدول النامية قد تفتقر إلى الموارد أو المعرفة للمشاركة بشكل فعال في التطورات التي تحصل في العالم. والسبب في ذلك عدم وجود قوانين دولية متفق عليها لتنظيم التكنولوجيا، مما يجعل من الصعب تنفيذ السياسات التنظيمية في مجال التكنولوجيا المتطورة. فالتعاون الدولي ينجح في هذا المجال ويزدهر مثل ما ازدهر غيره من قبل كالاتفاقيات حول الأسلحة النووية التي أبرمت عندما كان هنالك استعداد للتعاون بين الدول الكبرى أدى إلى إنشاء معاهدات مثل معاهدة عدم انتشار الأسلحة النووية (NPT). كذلك تأسيس منظمة الطيران المدني الدولي (ICAO) لتنسيق وتنظيم صناعة الطيران على مستوى العالم. والاتحاد الدولي للاتصالات (ITU) وهو منظمة تابعة للأمم المتحدة تنظم ترددات الراديو وشبكات الاتصالات[45]. اتفاقية باريس للمناخ (2015) تجمع دولي يهدف إلى الحد من ظاهرة الاحتباس الحراري بأستخدام التكنولوجيا النظيفة. فهي تعتمد على التزام الدول بالتعاون لتحقيق أهداف بيئية مشتركة. واللائحة العامة لحماية البيانات (GDPR) في الاتحاد الأوروبي تضع معايير صارمة لحماية الخصوصية في أوروبا، لكنها أثرت على الشركات العالمية وأصبحت نموذجاً يحتذى به. واتفاقية بودابست بشأن الجرائم الإلكترونية التي تعد أول معاهدة دولية تهدف إلى تعزيز التعاون بين الدول لمكافحة الجرائم الإلكترونية. ومنظمة الطيران المدني الدولي (ICAO) التي تنظم النقل الجوي على مستوى عالمي لضمان السلامة والأمن[46]. إن بناء الثقة بين الدول من خلال تبادل المعلومات والبيانات بشفافية ، لا شك بأنها تنعكس على تمكين الدول النامية خاصةً عند تقديم الدعم التكنولوجي والمالي لها لضمان مشاركتها الفعالة.

فالتعاون بين الحكومات والشركات التقنية الكبرى والدول النامية يخلق سياسات مشتركة تطوير خطة طويلة الأجل لتنظيم التكنولوجيا تشمل أهدافاً واضحة ومعايير زمنية. فتعزيز التعاون الدولي لتطوير آليات تنظيم عالمية أصبح ضرورة لضمان الاستخدام المسؤول للتكنولوجيا، وحماية حقوق الأفراد، وتعزيز الأمن والاستقرار العالمي . التعاون الناجح يتطلب رؤية مشتركة، إرادة سياسية قوية، واستعداداً لتجاوز الخلافات من أجل تحقيق الصالح العام. إن التعاون الدولي يعزيز الابتكار، ويضع معايير مشتركة يخلق بيئة أكثر استقراراً للشركات المبتكرة. ويعزيز الأمن العالمي فالتعاون في مجال الأمن السيبراني يقلل من خطر الهجمات العابرة للحدود. وكذلك تحقيق التنمية المستدامة إذ أن إستخدام التكنولوجيا لحل مشكلات عالمية مثل تغير المناخ والجو . ويعمل على تقليل الفجوة التكنولوجية ودعم الدول النامية يمكن أن يساهم في تقليل التفاوت التكنولوجي . فالتعاون الدولي لتطوير آليات تنظيم عالمية ليس مجرد ضرورة، بل هو شرط أساسي لضمان الاستخدام الآمن والعادل للتكنولوجيا. من خلال تعزيز الحوار، بناء الثقة، وتوحيد الجهود، يمكن للعالم مواجهة التحديات المشتركة وتحقيق مستقبل مستدام ومزدهر للجميع.

الخاتمة

لقد أصبح القانون الدولي أمام اختبار حقيقي في قدرته على الاستجابة لتلك التحديات. فالتطورات السريعة في مجالات مثل الذكاء الاصطناعي، الأمن السيبراني، وحوكمة الإنترنت تفرض ضرورة ملحة لتطوير أطر قانونية دولية تواكب هذه التحولات. وبينما يوفر القانون الدولي أدوات أساسية لتنظيم العلاقات بين الدول، فإن الحاجة إلى قواعد جديدة ومتكاملة للتعامل مع التحديات الرقمية أصبحت ضرورة لا غنى عنها لضمان الأمن، الاستقرار، والعدالة الرقمية. لذا فأن القانون الدولي يلعب دوراً حاسماً في مواجهة التحديات الرقمية المتزايدة ، لكن نجاحه يعتمد على مرونته وقدرته على التكيف مع متطلبات العصر. التعاون الدولي، الابتكار القانوني، وحماية حقوق الإنسان يجب أن تكون المحاور الرئيسية لأي جهود مستقبلية في هذا المجال. من خلال تكاتف الجهود وتوحيد الرؤى، يمكن للعالم ضمان نظام قانوني عادل وشامل يدعم التنمية الرقمية ويحمي استقرار المجتمع الدولي.

النتائج:-

1- إن التكنولوجيا الرقمية تتجاوز حدود السيادة الوطنية هي عابرة للحدود، مما يتطلب تنسيقاً دولياً أكثر فاعلية للتعامل مع القضايا المتعلقة بالأمن السيبراني والخصوصية.

2- إن تنامي الفجوة التنظيمية من خلال التطور التكنولوجي يفوق قدرة الأطر القانونية الحالية على التنظيم، مما يؤدي إلى فراغ قانوني تستغله أطراف غير مسؤولة.

3- إن تزايد الحاجة إلى تعزيز حماية حقوق الإنسان في الفضاء الرقمي ، بما في ذلك الحق في الخصوصية وحرية التعبير يمنحه ثقة كبيرة .

4- إن الهجمات السيبرانية والجرائم الإلكترونية أصبحت تهديداً للأمن الدولي، ما يجعل من الضروري تعزيز التعاون القانوني بين الدول.

5- التحديات الرقمية تتطلب قوانين ديناميكية ومرنة تواكب التطور السريع للتكنولوجيا.

التوصيات:-

1- تعزيز التعاون الدولي من خلال إنشاء منصات عالمية للحوار القانوني حول التحديات الرقمية، تضم الحكومات، القطاع الخاص، والمجتمع المدني.

2- تطوير معاهدات دولية جديدة تنظم الفضاء الرقمي وتحد من إساءة استخدام التكنولوجيا. وتعديل القوانين الدولية الحالية لتشمل قضايا جديدة مثل الذكاء الاصطناعي، العملات الرقمية.

3- تطوير معايير موحدة للتعامل مع الجرائم الإلكترونية وحوكمة البيانات.

4- إنشاء منظمات دولية متخصصة. وتأسيس هيئة دولية لتنظيم الذكاء الاصطناعي تشرف على تطبيق المبادئ الأخلاقية والتكنولوجية.

5- تشكيل مركز عالمي لمكافحة الجرائم السيبرانية يوفر الدعم الفني والقانوني للدول.

6- تقديم الدعم الفني والمالي للدول النامية لمساعدتها على مواجهة التحديات الرقمية. مع ضمان أن تكون أي مبادرات قانونية شاملة وفعّالة على المستوى العالمي.

7- وضع مواثيق دولية لحماية الخصوصية، حرية التعبير، وحقوق الإنسان في الفضاء الرقمي.إنشاء آليات رقابية تضمن احترام هذه الحقوق من قبل الحكومات والشركات.

8- تنظيم برامج تدريبية للقضاة والمحامين وأساتذة القانون الدولي العام والمختصين في فهم التحديات الرقمية. ودعم الأبحاث والدراسات القانونية المتعلقة بالتحول الرقمي.

الهوامش

(1) محمد بن مكرم بن منظور الأندلسي، لسان العرب، دار صادر،ط3، بيروت – لبنان، 1993، ج 4، ص 19.

(2) إبراهيم مصطفى وأخرون،المعجم الوسيط ،الجزء الأول ،مطبعه مصر ،القاهرة،1960،ص175.

(3) د.جعفر جاسم،حرب المعلومات بين أرث الماضي وديناميكية المستقبل، دار البداية للنشر والتوزيع،عمان،ط1، 2010.

(4) د.الحسيني عمار عباس،جرائم الحاسوب والانترنت الجرائم المعلوتية،ط1،منشورات زين الحقوقية،بيروت،لبنان،ب-د،ص98.

(5) د.إبراهيم طلال محمد الحاج،الهجمات الالكترونية على شبكات الحاسوب في ضوء القانون الدولي الإنساني، جامعة دمشق،كليه الحقوق قسم القانون الدولي،بحث منشور،2019،ص28.

(6) د.الحسيني عمار عباس، المصدر أعلاه،ص 126.

(7) زهراء رياض علي الطائي،مفهوم النزاع الالكتروني، بحث منشور على الرابط لالكتروني بتاريخ 2020 13/10/ https://portal.arid.my/16447/Posts/Detail.

(8) د.أحمدعلي، دراسات في القانون الدولي الإنساني، ط1، دار الأكاديمية، الجزائر، 2011، ص.68.

(9) أحمد عبد العليم، اللجنة الدولية للصليب الأحمر، 2004، ص49.

(10) د.صابرالقاسم ،الهجمات السيبرانية وموجهتها في ضوء القانون الدولي المعاصر،مجلة حقوق الانسان والحريات العامة،دار النهضة،2019،ص187.

(11) ياسمين عبد المنعم عبد الحميد، التحديات القانونية لتنظيم الذكاء الاصطناعي في، بحث منشور في المجلة القانونية، جامعة القاهرة، العدد8، 2020، ص 31.

(12) دليلة العوفي،الحرب السيبرانية في عصر الذكاء الاصطناعي ورهاناتها على الأمن الدولي، بحث منشور في مجلة الحكمة للدراسات الفلسفية، مؤسسة كنوز الحكمة، الجزائر، المجلد 9، 2021، ص79.

(13) أيمن محمد سيد مصطفى، النظام القانوني للبث الفضائي عبر الأقمار الصناعية،مركز الدراسات العربية،مصر،2019،ص46.

(14) د. محمود احمد عبابنة، جرائم الحاسوب وأبعادها الدولية،دار الثقافة للنشر،عمان،ص103.

(15) ينظر:تقرير اجتماع الخبراء لعام 2016 بشأن منظومات الأسلحة الفتاكة ذاتية التشغيل، المؤتمر الاستعراضي الخامس للأطراف المتعاقدة السامية في اتفاقية حظر استعمال الأسلحة التقليدية، رقم الوثيقة (CCW/CONF.V/2)، ص11.

(16) Russel Christian,AMoral and Legal Imperative To Ban Killer Robots,Geneva, 2018, P.29.

(17) Neha Jain ,Human Machine International in Terms of Various Degrees of Autonomy as Well as Political, Federal Foreign Office ,2018,p.28.

(18) زهراء عماد محمد،المسؤولية الدولية الناشئة عن الهجمات الالكترونية، دروب المعرفة، مصر،2018،ص44.

(19) زهراء عماد محمد،المصدر اعلاه،ص51.

(20) خالد حسن احمد لطفي، الذكاء الاصطناعي وحمايته من الناحية المدنية والجنائية، دار الفكر الجامعي،القاهرة، 2021،ص231.

(21)د. محمد عز الدين علي،حرب المعلومات في ظل عصر المعلومات،بحث منشور في مجلة الدراسات الإنسانية،جامعة دنقلا، السودان،عدد 2105،4 ص164.
(22)د.محمود محمد سويف،جرائم الذكاء الاصطناعي (المجرمون الجدد)، دار الجامعة الجديدة،مصر، 2022، ص 125.
(23)Human Rights Watch, Mind the Gap,The Lack of Accountability Killer Robots , printed in the United States ofAmerica ,2019 , P. 33.
(24)د.حمدان إيمان، التكنولوجيا الجديدة والقانون الدولي الإنساني،دار نشر المعرفة،الجزائر،2020، ص 119.
(25) Human Rights Watch, Op.Cit,p.126.
(26)خالد حسن احمد لطفي، المصدر أعلاه،ص78.
(27)Karin Ahrin,Lethal autonomous robots and theAccountability gap in international criminal law,Univercity of Gothenburg,Economics and Law , 2019 , p.31.
(28)د.حمدان إيمان، المصدر أعلاه،ص201.
(29)Danial,Autononomous Weapons and the Problem of Stste Accountability , Chicago Journal of International law , volume 15 , number 2 , Article 8 , 2015 ,p.66.
(30)د.ياسر محمد اللمعي،المسؤولية الجنائية عن أعمال الذكاء الاصطناعي،بحث منشور، مجلة كلية الحقوق، جامعة المنصورة،عدد خاص بالمؤتمر الدولي السنوي العشرون،2021، ص876.
(31)د. محمد عز الدين علي،مصدر سابق،ص28.
(32)د.حمدان إيمان، المصدر أعلاه،ص201.
(33) للمزيد زيارة الموقع الالكتروني للاطلاع على مضمون البيانات الخاصة باللائحة(GDPR) https://privacy.google.com/businesses
(34)د.ياسر محمد اللمعي، المصدر السابق ،878.
(35)أصدرت كاليفورنيا قانون خصوصية المستهلك، ودخل القانون حيز التنفيذ في 1 يناير 2020 ويعد CCPA أحد أكثر قوانين خصوصية البيانات شمولا في الولايات المتحدة. ويركز CCPA بشكل أساسي على حقوق المستهلك فيما يتعلق بجمع واستخدام البيانات الشخصية أو الخاصة. بموجبه يمكن لجميع سكان كاليفورنيا الآن ممارسة الحق في طلب جميع البيانات الخاصة التي قامت الشركة بتخزينها.للمزيد انظر .https://www.questionpro.com/security/ccpa
(36)رانيا صبحي محمد عزب،العقود الرقمية في قانون الإنترنت،دراسة تحليلية مقارنة في التشريعات العربية والأميركية والأوروبية، دار الجامعة الجديدة، مصر، 2012، ص 119.
(37) رانيا صبحي محمد عزب ،المصدر السابق ،ص159-165.
(38)د.حسام عبد الامير خلف، القتل المستهدف باستخدام الروبوتات الطائرات بدون طيار في القانون الدولي، بحث منشور في مجلة العلوم القانونية، كلية القانون، جامعة بغداد، مجلد29،عدد1، 2014، ص33.
(39)براء منذر كمال عبد اللطيف، الطائرات المسيرة من منظور القانون الدولي الإنساني، الكويت،2019،ص125.
(40)د.حسام عبد الامير خلف، المصدر السابق،ص55.
(41)ابو بكر محمد احمد الديب، قمع انتهاكات الطائرات المسلحة بلا طيار للقانون الدولي، بحث منشور في مجلة الدراسات القانونية والاقتصادية، كلية الحقوق،القاهرة،عدد 2،2021،ص53.
(42)د.حسام عبد الامير خلف ، المصدر اعلاه ، ص71.
(43)Stefan A. Kaiser Legal Aspects of Unmanned Aerial Vehicles - German Journal of Air and Space Law, Vol. 55, 2006.p34.
(44)Gordon Lubold, As Drones Multiply in Iraq and Afghanistan, So Do Their Uses,The Christian Science Monitor, March 2, 2010.p.203.
(45)https://www.bbc.com/arabic/scienceandtech.
(46)اليمامة خضير الحربي،جوانب قانونية في الحوكمة التكنولوجية للإنترنت،بحث منشور في مجلة كلية القانون الكويتية العالمية، الكويت، السنة السادسة، عدد4، 2018،ص98.

المصادر/ الكتب العربية/الكتب والبحوث.

1- إبراهيم مصطفى وأخرون،المعجم الوسيط ،الجزء الأول ،مطبعه مصر ،القاهرة،1960.
2- أحمد علي، دراسات في القانون الدولي الإنساني، ط1، دار الأكاديمية، الجزائر، 2011.
3- إبراهيم طلال محمد الحاج،الهجمات الالكترونية على شبكات الحاسوب في ضوء القانون الدولي الإنساني، جامعة دمشق،كليه الحقوق قسم القانون الدولي،بحث منشور،2019.
4- ابو بكر محمد احمد الديب، قمع انتهاكات الطائرات المسلحة بلا طيار للقانون الدولي، بحث منشور في مجلة الدراسات القانونية والاقتصادية، كلية الحقوق،القاهرة،عدد2 ،2021.

5- أحمد عبد العليم، اللجنة الدولية للصليب الأحمر، 2004.
6- الحسيني عمار عباس،جرائم الحاسوب والانترنت الجرائم المعلوماتية،ط1منشورات زين الحقوقية،بيروت،لبنان،ب-د.
7- أيمن محمد سيد مصطفى، النظام القانوني للبث الفضائي عبر الأقمار الصناعية،مركز الدراسات العربية،مصر،2019.
8- اليمامة خضير الحربي،جوانب قانونية في الحوكمة التكنولوجية للإنترنت ، بحث منشور في مجلة كلية القانون الكويتية العالمية، الكويت، السنة السادسة، عدد4، 2018.
9- براء منذر كمال عبد اللطيف، الطائرات المسيرة من منظور القانون الدولي الإنساني، الكويت،2019.
10- حمدان إيمان، التكنولوجيا الجديدة والقانون الدولي الإنساني،دار نشر المعرفة،الجزائر،2020.
11- خالد حسن احمد لطفي، الذكاء الاصطناعي وحمايته من الناحية المدنية والجنائية، دار الفكر الجامعي،القاهرة، 2021.
12- جعفر جاسم،حرب المعلومات بين أرث الماضي وديناميكية المستقبل، دار البداية للنشر والتوزيع،عمان،ط1، 2010.
13- حسام عبد الامير خلف، القتل المستهدف بأستخدام الطائرات بدون طيار في القانون الدولي، بحث منشور في مجلة العلوم القانونية، كلية القانون، جامعة بغداد، مجلد29،عدد1، 2014.
14- صابر القاسم ،الهجمات السيبرانية وموجهتها في ضوء القانون الدولي المعاصر،مجلة حقوق الانسان والحريات العامة ، دارالنهضة ، 2019.
15- دليلة العوفي،الحرب السيبرانية في عصر الذكاء الاصطناعي ورهاناتها على الأمن الدولي، بحث منشور في مجلة الحكمة للدراسات الفلسفية، مؤسسة كنوز الحكمة، الجزائر، المجلد9 ،2021.
16- زهراء عماد محمد،المسؤولية الدولية الناشئة عن الهجمات الالكترونية، دروب المعرفة، مصر،2018.
17- رانيا صبحي محمد عزب،العقود الرقمية في قانون الإنترنت،دراسة تحليلية مقارنة في التشريعات العربية والأميركية والأوروبية، دار الجامعة الجديدة، مصر، 2012.
18- محمود احمد عبابنة، جرائم الحاسوب وأبعادها الدولية،دار الثقافة للنشر،عمان، ب،د.
19- محمود محمد سويف،جرائم الذكاء الاصطناعي (المجرمون الجدد)، دار الجامعة الجديدة،مصر، 2022.
20- محمد عز الدين علي،حرب المعلومات في ظل عصر المعلومات،بحث منشور في مجلة الدراسات الإنسانية،جامعة دنقلا، السودان،عدد4 ،2105.
21- محمد بن مكرم بن منظور الأندلسي، لسان العرب، دار صادر،ط3، بيروت – لبنان، 1993.
22- ياسر محمد اللمعي،المسؤولية الجنائية عن أعمال الذكاء الاصطناعي،بحث منشور، مجلة كلية الحقوق، جامعة المنصورة،عدد خاص بالمؤتمر الدولي السنوي العشرون،2021.
23- ياسمين عبد المنعم عبد الحميد، التحديات القانونية لتنظيم الذكاء الاصطناعي، بحث منشور في المجلة القانونية، جامعة القاهرة، العدد ٨ ، ٢٠٢٠.

الكتب الأجنبية ومواقع الانترنيت:-

1- Danial,Autononomous Weapons and the Problem of Stste Accountability , Chicago Journal of International law , volume 15, 2015.
2- Gordon Lubold, As Drones Multiply in Iraq and Afghanistan, So Do Their Uses,The Christian Science Monitor, March 2, 2010.
3- Human Rights Watch, Mind the Gap,The Lack of Accountability Killer Robots , printed in the United States ofAmerica ,2019.
4- Karin Ahrin,Lethal autonomous robots and theAccountability gap in international criminal ,Univercity of Gothenburg,Economics and Law .
5- Russel Christian,AMoral and Legal Imperative To Ban Killer Robots,Geneva, 2018.
6- Neha Jain ,Human Machine International in Terms of Various Degrees of Autonomy as Well as Political, Federal Foreign Office ,2018.
7- Stefan A. Kaiser Legal Aspects of Unmanned Aerial Vehicles - German Journal of Air and Space Law, Vol. 55, 2006.
8- https://portal.arid.my/16447/Posts/Detail.
9- https://privacy.google.com/businesses.
10- https://www.questionpro.com/security/ccpa.
11- https://www.bbc.com/arabic/scienceandtech.