الملتقى الوطني حول الدبلوماسية الرقمية

1_ **الدكتورة الأخضري فتيحة** البريد الالكتروني : lfatiha360@gmail.com

كلية الحقوق والعلوم السياسية قسم الحقوق رقم الهاتف : 0658892055

جامعة غرداية

2_ **الدكتورة عثماني كريمة** البريد الالكتروني :**karima.atma@yahoo.fr**

0666093577

كلية الحقوق والعلوم السياسية قسم الحقوق رقم الهاتف :

جامعة ميرة عبد الرحمان بجاية

محور المشاركة : ضمانات نشاط الدبلوماسية الرقمية

عنوان المداخلة : مخاطر الدبلوماسية الرقمية

ملخص : يستعرض المقال الضمانات القانونية اللازمة لتنظيم وحماية النشاط الدبلوماسي في العصر الرقمي، مع التركيز على التهديدات السيبرانية التي تواجه البعثات الدبلوماسية في الفضاء الإلكتروني. يناقش المقال أهم الاتفاقيات الدولية مثل اتفاقية فيينا 1961 التي تنظم العلاقات الدبلوماسية، واتفاقية بودابست 2001 التي تتناول مكافحة الجرائم السيبرانية، ويؤكد على ضرورة تحديث هذه الاتفاقيات لتشمل الحماية الرقمية .الإشكالية تتمثل في غياب إطار قانوني شامل يواكب التحديات الرقمية المتزايدة، ما يجعل الأنشطة الدبلوماسية عرضة للمخاطر السيبرانية التي تهدد أمن المعلومات والعلاقات الدولية.

Summary :

This article discusses the legal guarantees necessary to regulate and protect diplomatic activities in the digital age, focusing on the cyber threats faced by diplomatic missions in cyberspace. It examines key international agreements, such as the 1961 Vienna Convention, which governs diplomatic relations, and the 2001 Budapest Convention, which addresses cybercrime. The article stresses the need to update these agreements to include digital protection. The **issue** revolves around the lack of a comprehensive legal framework that keeps up with increasing digital challenges, leaving diplomatic activities vulnerable to cyber risks that threaten information security and international relations.

مقدمة :

في ظل التحولات المتسارعة التي يشهدها العالم بفعل التطور التكنولوجي، أصبحت الرقمنة جزءاً لا يتجزأ من الحياة اليومية للدول والمؤسسات، بما في ذلك الأنشطة الدبلوماسية. فقد باتت الدبلوماسية الرقمية قناة أساسية للتواصل بين الدول، تُوظف من خلالها الحكومات أدوات التكنولوجيا الحديثة لتعزيز

الحوار، إدارة الأزمات، وتحقيق المصالح المشتركة. ومع ذلك، فإن هذه النقلة النوعية لم تخلُ من تحديات قانونية وأمنية، أبرزها التهديدات السيبرانية التي تستهدف البعثات الدبلوماسية والمنشآت الحساسة، مما يطرح إشكاليات قانونية تتعلق بضمان الحصانة الرقمية، حماية البيانات، والسيادة في الفضاء السيبراني.

هذه التحولات الرقمية في العمل الدبلوماسي أوجدت حاجة ملحّة لإعادة التفكير في الأطر القانونية التي تحكم هذا النشاط. فالعمل الدبلوماسي التقليدي كان محمياً بمجموعة من الاتفاقيات الدولية، مثل اتفاقية فيينا للعلاقات الدبلوماسية (1961)، التي أرست ضمانات قانونية للحصانات الدبلوماسية. غير أن البيئة الرقمية تستدعي مقاربات جديدة تأخذ بعين الاعتبار خصوصيات الفضاء السيبراني. غياب الإطار القانوني الدولي الموحد والتنظيم الدقيق لأنشطة الدبلوماسية الرقمية يخلق فراغاً قانونياً يعرّض البعثات والمؤسسات الدبلوماسية لمخاطر السيادة الرقمية والهجمات السيبرانية المتزايدة.

إن التحديات التي تواجهها الدبلوماسية الرقمية اليوم تتطلب ضمانات قانونية واضحة تشمل حماية البيانات الرقمية، تنظيم مسؤوليات الدول في الفضاء السيبراني، وتعزيز التعاون الدولي لمواجهة التهديدات المشتركة. هذا المقال يسعى لتسليط الضوء على هذه التحديات وتحليلها من منظور قانوني، مع تقديم حلول مبتكرة تدعم العمل الدبلوماسي الرقمي وتُحقق التوازن بين الفاعلية الرقمية واحترام القواعد الدولية، بما يضمن استمرارية العمل الدبلوماسي في العصر الرقمي وتحقيق أهدافه بفعالية وأمان.

المبحث الأول: الاتفاقيات الدولية ذات الصلة

تُعد الاتفاقيات الدولية أساساً قانونياً مهماً لتنظيم العمل الدبلوماسي وحمايته، ومن أبرزها اتفاقية فيينا للعلاقات الدبلوماسية (1961) التي أرست مبادئ الحصانة الدبلوماسية وحرمة المراسلات الرسمية. ومع التحول الرقمي، ظهرت الحاجة إلى توسيع هذه الضمانات لتشمل الأنشطة الرقمية. ورغم أن الفضاء السيبراني يفتقر إلى إطار قانوني شامل، فإن جهوداً دولية، مثل اتفاقية بودابست بشأن الجرائم السيبرانية (2001)وإرشادات تالين بشأن الحرب السيبرانية، توفر معايير مبدئية يمكن الاستناد إليها لتأمين وحماية الدبلوماسية الرقمية في مواجهة التحديات الحديثة.

المطلب الأول : اتفاقية بودابست لمكافحة الجرائم السيبرانية:(2001)

تعد اتفاقية بودابست الإطار القانوني الدولي الأساسي في مواجهة الجرائم السيبرانية. حيث توفر الاتفاقية مجموعة من التدابير التي تعزز أمن المعلومات الرقمية.

فمع الانتقال المتزايد للنشاط الدبلوماسي إلى الفضاء الرقمي، أصبحت البعثات الدبلوماسية تواجه تهديدات سيبرانية متصاعدة تشمل التجسس الرقمي، اختراق الخوادم، وسرقة البيانات الحساسة. في هذا السياق، توفر **اتفاقية بودابست لمكافحة الجرائم السيبرانية (2001)** إطارًا قانونيًا أساسيًا لتجريم هذه الممارسات، مستندة إلى نصوص واضحة مثل المادة 2، التي تجرم "الوصول غير المشروع إلى الأنظمة الحاسوبية"، والمادة 3، التي تجرم "اعتراض البيانات غير المشروع". هذه النصوص توفر أساسًا لحماية المعلومات الرقمية الدبلوماسية من الاختراقات غير المصرح بها. كما تسهم الاتفاقية في تأمين المراسلات الدبلوماسية، إذ تشير المادة 4 إلى "تجريم إساءة استخدام البيانات"، مما يضمن سلامة الاتصالات الإلكترونية للبعثات الدبلوماسية.

علاوة على ذلك، تعزز الاتفاقية التعاون الدولي من خلال المادة 23، التي تنص على "التعاون الدولي لتسليم المعلومات والمساعدة القانونية المتبادلة بين الدول"، مما يتيح آليات لتحديد المسؤولين عن الهجمات السيبرانية العابرة للحدود وملاحقتهم قضائيًا. يُعتبر هذا البند أحد أهم الأدوات لتعزيز الثقة بين الدول في إدارة التهديدات الرقمية المشتركة، بما يضمن حماية النشاط الدبلوماسي الرقمي في إطار بيئة

قانونية شاملة. كما تؤكد الاتفاقية من خلال المادة 24 على حق الدول في حماية بنيتها الرقمية من الأنشطة السيبرانية غير القانونية التي قد تُنفذ من أراضيها، مما يعزز مبدأ السيادة الرقمية ويسهم في خلق بيئة دبلوماسية آمنة.

ومع ذلك، تواجه الاتفاقية تحديات تحد من فعاليتها في حماية النشاط الدبلوماسي الرقمي. من أبرز هذه التحديات عدم شمولية الاتفاقية، حيث لم تصادق عليها بعض الدول الكبرى، مما يضعف من قدرتها على التصدي للتهديدات العالمية. بالإضافة إلى ذلك، يتطلب التطور التكنولوجي السريع وأساليب الهجوم السيبراني المتجددة مراجعة دائمة لمواد الاتفاقية لتواكب المستجدات. كما يؤدي أيضًا التداخل بين مقتضيات الأمن القومي وحماية الدبلوماسية الرقمية إلى استغلال بعض الدول للنصوص القانونية لتحقيق أهداف أمنية أوسع، مما قد يهدد خصوصية الدول الأخرى وسيادتها الرقمية.

بناءً على ذلك، تتضح الحاجة إلى توسيع نطاق عضوية الاتفاقية ودعوة الدول غير الموقعة إلى المصادقة عليها، وتحديث بنودها لتشمل صراحة حماية الأنشطة الدبلوماسية الرقمية. كما يُوصى بتفعيل المادة 35، التي تنص على "إنشاء نقاط اتصال على مدار الساعة لتقديم الدعم الفني والقانوني"، من خلال إنشاء مراكز متخصصة لتبادل الخبرات والتقنيات السيبرانية، مع تطوير بروتوكولات أمنية مخصصة لهذا المجال الحيوي.

وفي أوت 2024، تبنّت الأمم المتحدة أول معاهدة لها لمكافحة الجريمة السيبرانية بعد ثلاث سنوات من المفاوضات. تهدف هذه الاتفاقية إلى تعزيز التعاون الدولي في مواجهة الجرائم الإلكترونية، بما في ذلك تلك التي تستهدف البنية التحتية الحساسة أو تستغل الاتصالات الرقمية. تشمل المعاهدة عدة أحكام تتعلق بتبادل الأدلة الإلكترونية، وتعزيز القدرات التقنية للدول ذات البنية التحتية الأقل تطورًا.

وتمثل هذه المعاهدة تطورًا هامًا للدبلوماسية الرقمية، حيث توفر وسائل قانونية لمواجهة التهديدات السيبرانية التي قد تستهدف البعثات الدبلوماسية أو المراسلات الرسمية. ومع ذلك، أُثيرت مخاوف من قبل منظمات حقوق الإنسان وبعض شركات التكنولوجيا، إذ يُعتقد أن بعض أحكامها قد تُستخدم كأداة للتوسع في المراقبة وانتهاك الخصوصية، وهو ما يعكس تحديات التوازن بين الأمن الرقمي وحماية الحقوق الأساسية.

من ناحية أخرى، ارتبطت هذه المعاهدة بتقوية الجهود الدولية المبذولة في إطار اتفاقية بودابست لمكافحة الجرائم السيبرانية لعام 2001، حيث استُخدمت الأخيرة كمرجع قانوني في العديد من الأحكام. مع ذلك، تتسم المعاهدة الجديدة بأبعاد أوسع تشمل بنودًا إضافية تهدف إلى تعزيز التعاون القضائي الدولي، مع الإصرار على احترام حقوق الإنسان كجزء من النصوص القانونية الخاصة بها.

المطلب الثاني : اتفاقية فيينا للعلاقات الدبلوماسية:(1961)

رغم أنه تم إبرام هذه الاتفاقية في فترة سبقت عصر الرقمنة، تظل حجر الزاوية في تنظيم العلاقات بين الدول في سياقها التقليدي، وتوفر أسسًا قابلة للتطبيق على الدبلوماسية الرقمية الحديثة. فهذه الاتفاقية، التي أقرَّت المبادئ الأساسية للعلاقات الدبلوماسية، تُظهر قدرة فريدة على التكيف مع التحديات المعاصرة التي فرضها الانتقال إلى الفضاء الرقمي.

أولا : حماية المراسلات الدبلوماسية:

إذ تنص المادة 27 من الاتفاقية على أنه "يجب أن تتم حماية وسائل الاتصال الدبلوماسي". كان هذا المبدأ أساسًا لحماية البريد الدبلوماسي الورقي في زمنها، لكن مع تحول الأنشطة الدبلوماسية إلى الرقمية، يُمكن توسيع هذا المبدأ ليشمل الوسائل الرقمية الحديثة مثل البريد الإلكتروني، الرسائل المشفرة، والتطبيقات

الرقمية المخصصة. على ضوء ازدياد التهديدات السيبرانية التي تطال الدول في مختلف أنحاء العالم، تبرز الحاجة إلى حمايتها من هجمات قرصنة قد تؤثر على المعلومات الحساسة. ومن هذا المنطلق، يمكننا اعتبار المادة 27 بمثابة حجر الزاوية لحماية المراسلات الرقمية في عصرنا، وضمان سرية وأمن تدفق المعلومات بين البعثات الدبلوماسية.

ثانيا : الحصانات الدبلوماسية:

تعزز المادة 31 من الاتفاقية حصانة موظفي البعثات الدبلوماسية، بما يشمل حماية البيانات والمعلومات المستخدمة في أنشطتهم. إذا كانت الحصانات القانونية التقليدية تهدف إلى حماية الأفراد من الملاحقات القانونية، فإنها الآن تحتاج إلى التأقلم مع التحديات الرقمية. بمعنى آخر، يجب أن تشمل هذه الحصانة الأنظمة الإلكترونية والبنى التحتية الرقمية التي تستخدمها البعثات في نقل المعلومات، مما يعني حماية الخوادم، قواعد البيانات، والأنظمة السحابية التي تخزن معلومات دبلوماسية حساسة. فيُعد هذا تطورًا طبيعيًا من الحماية التقليدية إلى حماية عالمية تشمل الفضاء الرقمي.

ثالثا: الثغرات القانونية وإشكاليات التكيف مع العصر الرقمي:

إحدى الثغرات البارزة في اتفاقية فيينا هي غياب إشارة صريحة إلى المجال الرقمي. رغم أنها تتضمن أحكامًا قوية لحماية المراسلات والحصانات، إلا أن الاتفاقية لا تتناول بشكل تفصيلي التحديات التي تطرأ على العالم الرقمي، مثل الهجمات السيبرانية، تسريب البيانات، أو التهديدات المرتبطة بالتقنيات الحديثة كالتشفير أو الذكاء الاصطناعي. في هذا السياق، يصبح من الضروري تعديل الاتفاقية أو إضافة ملاحق جديدة تشمل بنودًا خاصة بالتكنولوجيا الرقمية وحمايتها. يمكن لهذه التعديلات أن تتيح للدول ضمان أمان أجهزتها وبياناتها ضد الهجمات الإلكترونية التي تستهدف النشاط الدبلوماسي.

إن التطبيق الحديث لهذه المبادئ يتطلب إعادة تعريف مصطلحات "التواصل الدبلوماسي" و"الحصانة" لتشمل الأبعاد الرقمية الجديدة. ربما يمكن إضافة مفاهيم جديدة مثل "الأنظمة الدبلوماسية الرقمية" و"الأمن السيبراني الدبلوماسي"، مما يعكس تطورًا في فهم الحماية القانونية التي يجب أن تحيط بالنشاط الدبلوماسي في العالم الرقمي. علاوة على ذلك، يمكن تطوير آليات قانونية خاصة بمعالجة القضايا المتزايدة المرتبطة بالجرائم السيبرانية العابرة للحدود، والتي تستهدف بعثات دبلوماسية عبر الإنترنت، كما يمكن توفير آليات خاصة للاستجابة الفورية للهجمات السيبرانية، مما يعزز الاستجابة العالمية الموحدة لتحديات العصر الرقمي.

وتجدر الإشارة إلى أن اتفاقية بودابست لمكافحة الجرائم السيبرانية (2001) و**اتفاقية فيينا للعلاقات الدبلوماسية (1961)** ليستا سوى نماذج مختصرة ضمن مجموعة واسعة من الاتفاقيات الدولية التي تهدف إلى تنظيم العلاقات بين الدول في عصر الرقمنة وضمان حماية النشاطات الدبلوماسية. هذه الاتفاقيات تمثل أسسًا قانونية تعالج القضايا المتعلقة بالأمن الرقمي وحماية المعلومات في فضاء العلاقات الدولية. فبينما توفر اتفاقية بودابست إطارًا قانونيًا لمكافحة الجرائم السيبرانية، تضمن اتفاقية فيينا حصانة وحماية الوسائل التقليدية للاتصال الدبلوماسي، والتي يمكن توسيعها لتشمل القنوات الرقمية الحديثة.

إلى جانب هاتين الاتفاقيتين، هناك العديد من الاتفاقيات الأخرى التي تم تبنيها في السنوات الأخيرة لضمان أمن الفضاء الرقمي، مثل **اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية** التي أُبرمت في 2024، وكذلك المبادرات الإقليمية التي تهدف إلى تعزيز التعاون بين الدول لمواجهة التهديدات الرقمية العابرة للحدود. جميع هذه الاتفاقيات تتكامل في تعزيز الإطار الدولي لحماية الأنشطة الدبلوماسية من المخاطر الرقمية المتزايدة، وهي ضرورية لضمان استقرار العلاقات الدولية في ظل تطور تكنولوجيا المعلومات والاتصالات.

المبحث الثاني: التهديدات السيبرانية وتأثيرها على النشاط الدبلوماسي

تواجه الأنشطة الدبلوماسية اليوم تهديدات متزايدة من الهجمات السيبرانية التي تستهدف البنية التحتية الرقمية للبعثات الدبلوماسية، ما يهدد أمن المعلومات والاتصالات الدولية. هذه التهديدات تُعقد العلاقة بين الدول وتفرض تحديات قانونية وأمنية جديدة، مما يستدعي وضع آليات قانونية وتقنية لحماية الدبلوماسية الرقمية.

المطلب الأول: الجرائم السيبرانية ضد السفارات والإجراءات الأمنية

تعد الجرائم السيبرانية التي تستهدف السفارات من أبرز التهديدات التي تواجه الدبلوماسية الرقمية. تشمل هذه الجرائم الهجمات على الأنظمة الإلكترونية والمراسلات المشفرة، مما يعرض الأمن القومي والمعلومات الحساسة للخطر. يتطلب التصدي لهذه الجرائم تطوير إجراءات أمنية متكاملة تُعزز الحماية السيبرانية للبعثات الدبلوماسية وتضمن الامتثال للقوانين الدولية ذات الصلة.

أولا : التهديدات السيبرانية التي تتعرض لها السفارات:

في عصر الرقمنة المتسارع، أصبحت السفارات والبعثات الدبلوماسية في مختلف أنحاء العالم عرضة لمجموعة متنوعة من التهديدات السيبرانية التي تشمل الهجمات الإلكترونية المتقدمة والتجسس الرقمي، مما يضع الأنظمة الأمنية والبيانات الحساسة الخاصة بها في خطر بالغ. هذه التهديدات تتنوع من الهجمات المنظمة التي تستهدف سرقة المعلومات إلى العمليات الموجهة التي تهدف إلى اختراق الأنظمة الدفاعية.

1. **الاختراقات الإلكترونية** :تشهد السفارات بشكل متزايد عمليات اختراق تهدف إلى التسلل إلى الشبكات الداخلية وسرقة أو تعديل البيانات الحساسة. تتنوع أساليب الاختراق من الهجمات عبر البرمجيات الخبيثة (Malware)التي تصيب الأنظمة لتُجري تحكمًا كاملاً عليها، إلى الهجمات بواسطة الفدية التي تهدد بتشفير البيانات المهمة إلا إذا تم دفع فدية. التقارير الأمنية مثل "The 2023 Cybersecurity Report"الصادر عن شركة كاسبرسكي تشير إلى أن السفارات هي واحدة من الأهداف الأساسية للهجمات الإلكترونية المعقدة، نظرًا لكونها حاضنة للمعلومات ذات القيمة الاستراتيجية والسياسية.
2. **التجسس الإلكتروني:** من جهة أخرى، تعد الهجمات التي تهدف إلى التجسس الإلكتروني واحدة من أخطر التهديدات التي تواجهها السفارات. في هذا النوع من الهجمات، يسعى المهاجمون إلى اختراق الشبكات الدبلوماسية للحصول على معلومات استراتيجية، سياسية، أو حتى تجارية قد تكون مؤثرة على العلاقات بين الدول. تُستخدم تقنيات مثل البرمجيات التجسسية (Spyware)و الهاكرز الموجهين لاختراق الأنظمة الرقمية للبعثات الدبلوماسية. تقارير من المركز الأوروبي للبحوث حول الأمن السيبراني تشير إلى أن الهجمات الموجهة ضد السفارات تعد وسيلة متقدمة لجمع المعلومات الحساسة التي تؤثر على المفاوضات السياسية بين الدول.

ثانيا : الإجراءات الأمنية المطلوبة:

في مواجهة هذه التهديدات المتزايدة، يجب على السفارات وضع إجراءات أمنية رقمية متقدمة للحفاظ على سرية المعلومات وحمايتها من الهجمات السيبرانية. تشمل هذه الإجراءات:

- التشفير المتقدم للبيانات :ينبغي تشفير جميع الرسائل والمراسلات الرقمية باستخدام خوارزميات التشفير ذات الحماية العالية مثل AES-256لضمان أن أي محاولة للوصول إلى المعلومات ستكون غير مجدية.
- أنظمة الدفاع ضد الهجمات :يجب تعزيز السفارات بأنظمة حديثة للكشف عن الهجمات مثل أنظمة الكشف عن التسلل (IDS) و الجدران النارية المتقدمة التي تمنع المهاجمين من اختراق الشبكات.
- المصادقة المتعددة العوامل :(MFA) يجب على السفارات تنفيذ تقنيات المصادقة متعددة العوامل لزيادة مستوى الأمان في الدخول إلى الأنظمة الحساسة.
- التدريب المستمر :وفقًا لتقرير "Global State of Cybersecurity 2024"الصادر عن منتدى الأمن السيبراني العالمي، يتعين على موظفي السفارات أن يتلقوا تدريبًا دوريًا حول أحدث أساليب الهجمات السيبرانية وكيفية التصدي لها، بالإضافة إلى الوعي حول الاستخدام الآمن للتكنولوجيا الرقمية.

ثالثا: التعاون الدولي وتنسيق الجهود.

نظرًا للطابع العابر للحدود للتهديدات السيبرانية، يصبح التعاون الدولي أمرًا بالغ الأهمية. في هذا الإطار، فلقد تطورت العديد من الاتفاقيات الدولية مثل اتفاقية بودابست لمكافحة الجرائم السيبرانية (2001)و اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية (2024)التي تشجع الدول على تعزيز التعاون في مواجهة هذه التهديدات. هذه الاتفاقيات باتت توفر أطرًا قانونية للتعاون بين الدول في التحقيق في الجرائم السيبرانية وملاحقة المهاجمين.

حيث أنه من خلال تنفيذ هذه الإجراءات الأمنية، وتعزيز التنسيق بين الدول، يمكن للسفارات أن تحمي نفسها بشكل فعال من التهديدات السيبرانية التي تهدد استقرار الأمن الدولي.

المطلب الثاني : مسؤولية الدول عن الأنشطة الرقمية.

في عصر تتسارع فيه وتيرة التحول الرقمي، تبرز مسؤولية الدول في مراقبة وتنظيم الأنشطة السيبرانية التي تنطلق من أراضيها أو تستخدم بنيتها التحتية. هذه المسؤولية تتطلب إعادة النظر في الأطر القانونية القائمة، بالنظر إلى تعقيد التحديات المرتبطة بالسيادة الرقمية، وضمان حماية الفضاء السيبراني من الاستغلال الضار، مع تحديد آليات تنسيق فعالة بين الدول لمواجهة تهديدات الأنشطة الرقمية العابرة للحدود.

أولاً: مبدأ السيادة الرقمية وحدود المسؤولية الدولية

في عصر تكنولوجيا المعلومات والاتصالات، أصبحت السيادة الرقمية بُعداً جديداً من السيادة التقليدية، لكنها تطرح تساؤلات معقدة حول مدى مسؤولية الدول عن الأنشطة السيبرانية التي تُنفذ من أراضيها أو عبر بنيتها التحتية. فالسيادة الرقمية ليست مجرد حق بل مسؤولية، تستوجب التزام الدول بمنع استخدام فضائها السيبراني لشن أعمال عدائية أو غير مشروعة ضد الآخرين. هذه المسؤولية تُؤطرها المادة 2 من ميثاق الأمم المتحدة ومشروع مواد مسؤولية الدول عن الأفعال غير المشروعة (2001). ومع ذلك، يظل الإطار القانوني الدولي غامضاً فيما يتعلق بردود الفعل على الهجمات السيبرانية، لا سيما تلك التي تستهدف المنشآت الدبلوماسية. على سبيل المثال، إرشادات تالين بشأن الحرب السيبرانية تقترح معايير

تنظيمية لكنها تفتقر إلى الصفة الإلزامية، مما يُبقي النقاش القانوني مفتوحاً حول حدود تطبيق قواعد الحرب التقليدية على الفضاء السيبراني.

ثانياً: الحصانات الرقمية وضرورة توحيد التشريعات الدولية

في ظل تحول العمل الدبلوماسي نحو الرقمنة، باتت الحصانات الدبلوماسية تمتد لتشمل الأجهزة والبيانات الرقمية، مما يطرح مفهوم "الحصانات الرقمية" كحق غير قابل للانتهاك .اتفاقية فيينا للعلاقات الدبلوماسية (1961) تؤكد على حرمة الوثائق والمراسلات، وهو ما يُمكن توسيعه ليشمل الحماية الرقمية. ومع ذلك، تُظهر الممارسات الدولية تناقضاً صارخاً؛ حيث تقوم بعض الدول بانتهاك هذه الحصانات تحت ذرائع مثل الأمن القومي، مما يُهدد النظام القانوني الدولي. بالإضافة إلى ذلك، فإن التفاوت التشريعي بين الدول فيما يتعلق بالأمن السيبراني يُمثل فجوة خطيرة تُستغل من قبل الجهات المعادية. ورغم الجهود الدولية مثل اتفاقية بودابست بشأن الجرائم السيبرانية، لا تزال الحاجة مُلحة لإطار قانوني عالمي يُعزز مفهوم المسؤولية المشتركة ويُعيد صياغة القواعد لضمان حماية الأنشطة الرقمية الدبلوماسية.

و لتحقيق العدالة السيبرانية، يمكن تطوير مفهوم "التكامل السيادي الرقمي"، وهو مبدأ جديد يضمن التزام الدول بمسؤولياتها الرقمية، مع توحيد الجهود الدولية لإرساء قواعد مُلزمة تحمي الحصانات الرقمية وتُجرّم الانتهاكات السيبرانية، بما يُعيد تشكيل قواعد القانون الدولي لمواكبة متطلبات العصر الرقمي.

الخاتمة

ختامًا، تُعد ضمانات النشاط الدبلوماسي الرقمي حجر الزاوية في حماية العلاقات الدولية في عصر تتزايد فيه التهديدات السيبرانية. إن تطوير إطار قانوني شامل وفعال يحمي النشاط الدبلوماسي الرقمي أصبح ضرورة ملحة لضمان استقرار وأمن هذه الأنشطة. وفي ضوء ما سبق، نقدم التوصيات التالية لتطوير وتعزيز العمل الدبلوماسي الرقمي وحمايته:

1. **تعزيز مفهوم "السيادة الرقمية المسؤولة:"**
   - وضع تعريف دولي موحد للسيادة الرقمية يشمل التزامات الدول بمنع استخدام فضائها السيبراني في شن هجمات على المنشآت الدبلوماسية أو انتهاك الحصانات الرقمية.
   - دعوة الدول لاعتماد مبدأ "المسؤولية المشتركة" في تأمين الفضاء الرقمي الدولي.
2. **تطوير إطار دولي للحصانات الرقمية:**
   - توسيع مفهوم الحصانات الدبلوماسية ليشمل الأجهزة الرقمية والبيانات المشفرة بموجب اتفاقية فيينا للعلاقات الدبلوماسية.(1961)
   - إنشاء آليات قانونية دولية لمحاسبة الدول التي تنتهك الحصانات الرقمية.
3. **اعتماد "ميثاق عالمي للأمن السيبراني الدبلوماسي:"**
   - صياغة ميثاق دولي جديد ينظم النشاط الرقمي الدبلوماسي، ويشمل قواعد حماية البعثات الدبلوماسية وآليات لتبادل المعلومات حول التهديدات السيبرانية.
4. **إنشاء هيئة دولية لمراقبة النزاعات السيبرانية:**

- تأسيس هيئة تابعة للأمم المتحدة تُعنى بالنزاعات الرقمية بين الدول وتوفير آليات للتحكيم وحل النزاعات وفقاً للقانون الدولي.

5. تعزيز التعاون الإقليمي والدولي:

- تشجيع الدول على الانضمام إلى اتفاقيات دولية مثل اتفاقية بودابست بشأن الجرائم السيبرانية.

6. إطلاق مبادرة "التكامل السيادي الرقمي:"

- اقتراح مفهوم "التكامل السيادي الرقمي" الذي يهدف إلى توحيد الجهود الدولية لتعزيز الأمن السيبراني في المجال الدبلوماسي.

7. تمكين الدبلوماسية الوقائية الرقمية:

- استخدام الأدوات الرقمية لرصد التهديدات السيبرانية قبل وقوعها وتعزيز منصات التعاون الدبلوماسي الرقمي بين الدول.

8. تعزيز الشفافية الدولية:

- دعوة الدول لنشر تقارير دورية حول الجهود التي تبذلها لتأمين فضائها السيبران.

قائمة المراجع

باللغة العربية

1. أحمد الجوهري، "الجرائم السيبرانية وسبل مكافحتها: دراسة مقارنة"، الدار العربية للعلوم ناشرون، 2017.
2. سعيد بوبكر، "الحق في الخصوصية في عصر الرقمنة"، مؤسسة شباب الجامعة، 2020.
3. محمد سليمان، "الأمن السيبراني وحماية البنية التحتية الحيوية: التحديات والفرص"، دار الفكر العربي، 2021.
4. يوسف أكرم عوض، "الأنظمة القانونية لحماية المعلومات الرقمية في القانون الدولي"،)جامعة القاهرة، 2023.
5. فوزية عبدالكريم، "مستقبل العلاقات الدولية في عصر الرقمنة: دراسة تحليلية في ضوء التحديات القانونية والسيبرانية"، مجلة الدراسات القانونية، 2021.

المراجع الأجنبية :

- Vázquez, C. (2007). The Legal Framework for Diplomacy. Oxford University Press.
- Hampson, F. (2014). International Law and Diplomacy in the Digital Age. Cambridge University Press.
- Weiss, T. G. (2015). The Diplomacy of Digital Transformation: International Norms in the Cyber Era. Palgrave Macmillan.

- Brouwer, E. (2019). Cybersecurity and International Law: A Study of the Budapest Convention and its Application to Diplomatic Communications. PhD Dissertation, University of Amsterdam.
- Mory, S. (2020). Digital Diplomacy: The Role of International Legal Instruments in Securing Diplomatic Communications. Master's Thesis, Harvard Law School.
- UNODC (2024). United Nations Convention on Cybercrime: A New Era of International Cooperation. United Nations Office on Drugs and Crime.
- "The Role of the Vienna Convention in Modern Diplomatic Protection", International Relations Journal, 2022, Vol. 16, Issue 3.
- "The Budapest Convention: A Legal Framework for Cybercrime Prevention", Cyberlaw Review, 2021.
- Council of Europe. (2001). Convention on Cybercrime (Budapest Convention). Council of Europe Treaty Series No. 185.
- NATO Cooperative Cyber Defence Centre of Excellence. (2017). Tallinn Manual on the International Law Applicable to Cyber Warfare.
- The Law of Cybercrime by Stephen B. Jones (2023). Oxford University Press.
- International Cybersecurity Law by Michael A. H. Armstrong (2022). Routledge.

Kulesza, J. (2016). International Law and the Future of Digital Diplomacy. Oxford University Press.

- Kiss, P. (2023). Cybersecurity Measures for Diplomatic Missions: Policy and Legal Perspectives. International Cyber Security Institute.
- Cybersecurity and International Diplomacy: A Critical Analysis by A. Patel, published in Global Diplomacy Review 2024.
- Legal Dimensions of Cyberattacks on Diplomatic Missions by M. F. Nguyen, published in Journal of International Legal Studies, 2023