

دور الحماية الدبلوماسية في عصر التحول الرقمي

**The Role of diplomatic protection
in the age of digital transformation**حصباية أحمد¹، د. عمران عائشة²¹ محبر الحقوق والعلوم السياسية، جامعة عمار ثليجي، الأغواط، البريد الإلكتروني: a.hasbaia@lagh-univ.dz² محبر الحقوق والعلوم السياسية، جامعة عمار ثليجي، الأغواط، البريد الإلكتروني: a.omrane@lagh-univ.dz

تاريخ النشر: 2025/04/20

تاريخ القبول: 2025/04/12

تاريخ الاستلام: 2025/02/06

ملخص:

في العقود الأخيرة، شهد العالم تحولاً رقمياً واسع النطاق أثر على جميع جوانب الحياة. فقد أصبحت التكنولوجيا الرقمية جزءاً لا يتجزأ من الأنظمة الاقتصادية، والسياسية، والاجتماعية، مما أدى إلى تغييرات جذرية في طريقة تفاعل الأفراد والدول مع بعضهم البعض. ومع زيادة الاعتماد على البيانات الرقمية والبنية التحتية السيبرانية، ظهرت تحديات جديدة تتعلق بالأمن، والخصوصية، والسيادة الرقمية. في هذا السياق، تبرز أهمية الحماية الدبلوماسية كوسيلة فعالة لحماية مصالح الرعايا والمواطنين في الخارج، خاصة في مواجهة المخاطر الناجمة عن الاستخدام السيئ للتكنولوجيا الرقمية. ولضمان استقرار العلاقات الدولية وتأمين المصالح الوطنية في ظل التحولات الرقمية المتسارعة.

كلمات مفتاحية: الحماية الدبلوماسية، التحول الرقمي، الهجمات السيبرانية، الرعايا الأجانب،

Abstract:

In recent decades, the world has witnessed a large-scale digital transformation that has affected all aspects of life. Digital technology has become an integral part of economic, political and social systems, leading to dramatic changes in the way individuals and states interact with each other. With greater reliance on digital data and cyber infrastructure, new security, privacy and digital sovereignty challenges have emerged. In this context, diplomatic protection is important as an effective means of protecting the interests of nationals and citizens abroad, especially in the face of risks arising from the poor use of digital technology. To ensure the stability of international relations and national interests in the context of accelerated digital transformations.

Keywords: Diplomatic protection, digital transformation, cyberattacks, foreign nationals

في ظل التحديات الرقمية المتزايدة، تواجه الدول هجمات إلكترونية متكررة تستهدف أنظمتها الحساسة، ما يهدد استقرارها الداخلي وأمنها القومي. كذلك، فإن الاعتماد على التكنولوجيا يفرض ضرورة التعاون الدولي لتأمين الفضاء السيبراني وحماية المصالح الوطنية والدولية.

وفي سياق التحول الرقمي السريع الذي يشهده العالم، تصبح الحماية الدبلوماسية أداة محورية لحماية الرعايا والمواطنين ولضمان استقرار العلاقات الدولية وحماية المصالح الوطنية في مواجهة التحديات السيبرانية المتزايدة. إن أهمية الموضوع لا تقتصر على الجوانب التقنية فقط، بل تمتد لتشمل أبعاداً قانونية وأخلاقية تعكس مدى ضرورة التعاون الدولي في هذا المجال. ولكون البحث في التحول الرقمي ليس فقط مهمًا لمواكبة التطورات التكنولوجية الحديثة، بل هو أيضًا ضروري لضمان أن هذه التطورات، إذا أُستُخدم بشكل فعال لتحقيق فوائد ملموسة للأفراد والمجتمعات والمؤسسات، في جميع الميادين والتخصصات.

حيث يتطلب المستقبل جهودًا منسقة لتطوير أطر قانونية شاملة، وتعزيز الثقة بين الدول، وتوظيف التكنولوجيا المتقدمة لضمان أمن الفضاء الرقمي. لذا، يبقى البحث والدراسة في هذا الموضوع ضرورة حتمية لضمان تحقيق توازن عادل بين التطور الرقمي والحفاظ على الحقوق السيادية والإنسانية. وتكمن أهمية الموضوع كذلك في كونه يواكب التطور التكنولوجي الذي بدأ يهيمن على أغلب مفاصل الحياة اليومية، للشعوب والمجتمعات، والذي يرافقه تحول عمل الأفراد، الدول والحكومات إلى نمط الحوكمة الإلكترونية، ومواكبة التغيرات المتعلقة به، على جميع الأصعدة، المحلية والإقليمية والدولية، وفي جميع الميادين.

ونظراً لتزايد تأثير التكنولوجيات الحديثة لاسيما الفضاء السيبراني والذكاء الاصطناعي على وضعية حقوق الإنسان وحرياته، ومن ثم على الأمن الدولي، كان من الأهمية بمكان، تبيان موقف منظمة الأمم المتحدة أيضاً وأجهزتها المختلفة ذات الصلة بحقوق الإنسان، إزاء الانعكاسات السلبية لتوظيف التكنولوجيا، ولجوء الدول إلى الحروب السيبرانية، أو استخدام القوة الإلكترونية بذريعة الدفاع الشرعي عن النفس أو محاربة الإرهاب، وكذا رؤية ميثاق الأمم المتحدة لمسألة حفظ السلم والأمن الدوليين التي يمكن أن تثيرها تلك التهديدات.

وكنتيجة للتحول الرقمي المتسارع، أصبحت التحديات القانونية المتعلقة بحماية حقوق الأفراد أكثر تعقيداً، خاصة مع توسع نطاق الجرائم الإلكترونية، وانتهاك الخصوصية، والرقابة الرقمية العابرة للحدود. في هذا السياق، تبرز إشكالية الحماية الدبلوماسية كوسيلة قانونية تقليدية وذات أصول عرفية ثابتة لحماية حقوق الأفراد في مواجهة الانتهاكات التي قد يتعرضون لها في الدول الأجنبية، مما يثير تساؤلات حول مدى فاعليتها في عصر الرقمنة والتداخل السيبراني.

وباتباع المنهج الوصفي، التحليلي سنحاول من خلال هذه الدراسة معالجة الإشكالية التالية: ما الدور الذي يمكن أن تؤديه الحماية الدبلوماسية في ضمان أمن المصالح الوطنية والدولية في سياق التحولات الرقمية المعاصرة؟

وذلك وفق المحاور الأربعة التالية:

- المحور الأول: مفهوم الحماية الدبلوماسية في السياق الرقمي
- المحور الثاني: تحديات التحول الرقمي على المستوى الدولي
- المحور الثالث: أهمية الحماية الدبلوماسية في مواجهة التحديات الرقمية
- المحور الرابع: مستقبل الحماية الدبلوماسية في عصر الرقمنة

المحور الأول: مفهوم الحماية الدبلوماسية في السياق الرقمي

تُعرف الحماية الدبلوماسية بأنها الإجراء الذي تتخذه دولة ما لحماية حقوق ومصالح مواطنيها¹ أو كياناتها القانونية في مواجهة انتهاكات تتعرض لها من قبل دولة أخرى، وذلك استناداً إلى القانون الدولي. تهدف الحماية الدبلوماسية إلى ضمان العدالة وتعويض الأضرار التي قد تلحق بالأفراد أو الشركات في الخارج، وهي أداة أساسية للحفاظ على الاستقرار في العلاقات الدولية.

وتُعد الحماية الدبلوماسية من المفاهيم الأساسية في القانون الدولي العام، حيث تمنح الدولة الحق في التدخل لحماية مواطنيها عندما تنتهك دولة أخرى حقوقهم بشكل جسيم. تستند هذه الحماية إلى مبدأ المسؤولية الدولية للدول²، إذ يحق للدولة المطالبة بإنصاف رعاياها إذا فشلت الدولة التي يقيمون فيها في توفير العدالة لهم، وفق مبدأ استنفاد سبل الانصاف الداخلية³. في هذا الإطار، ترتبط الحماية الدبلوماسية ارتباطاً وثيقاً بحقوق الإنسان، التي تعتبر حديثة العهد مقارنة بالحماية الدبلوماسية، حيث تُستخدم هذه الأخيرة كوسيلة لحماية الرعايا في الدول الأجنبية من الانتهاكات الجسيمة، مثل التعذيب، الاعتقال التعسفي، أو الحرمان من المحاكمة العادلة⁴. ومع تطور القانون الدولي لحقوق الإنسان، أصبحت هناك آليات أخرى مكملّة للحماية الدبلوماسية، مثل اللجوء إلى الهيئات الدولية كالمحكمة الأوروبية لحقوق الإنسان ولجان الأمم المتحدة. رغم ذلك، لا تزال الحماية الدبلوماسية أداة مهمة تضمن احترام حقوق الرعايا الطبيعيين والاعتباريين في الخارج،

¹ . عرف الفقيه بورشارد " Borchard " الحماية الدبلوماسية بوصفها الإجراء الذي تتقدم به دولة ما ضد دولة أخرى بشأن الأضرار التي يتعرض لها رعاياها، وقد ورد هذا التفسير في تقريره المقدم إلى معهد القانون الدولي عام 1931 عن الحماية الدبلوماسية للمواطنين في الخارج. حيث اقتصر على دراسة شروط الحماية في حالة تقديم طلب رسمي دولي، وهو ما اعتبره البعض تفسيراً شكلياً للحماية الدبلوماسية.

² . زازة لخضر، أحكام المسؤولية الدولية في ضوء قواعد القانون الدولي العام، دار الهدى للطباعة والنشر والتوزيع، الجزائر، 2011، ص 372.

³ . فوزي أوصديق، مبدأ التدخل والسيادة لماذا؟ وكيف؟، دار الكتاب الحديث، الجزائر، 1999، ص 288.

⁴ . العهد الدولي الخاص بالحقوق المدنية والسياسية، المادة 7 وما بعدها

مما يعكس تداخل القانون الدولي العام مع القانون الدولي لحقوق الإنسان في تعزيز العدالة وضمان كرامة الإنسان على المستوى الدولي¹.

وقد أحدث التحول الرقمي تغيرات جوهرية في العلاقات الدبلوماسية، وأثر تأثيراً مباشراً على نظام الحماية الدبلوماسية، حيث باتت التكنولوجيا تلعب دوراً محورياً في تسهيل التواصل بين الدول، وإدارة البيانات، واتخاذ القرارات. كما أدى إلى ظهور الدبلوماسية الرقمية² الجديدة تُستخدم فيها الأدوات والتكنولوجيا الرقمية لتعزيز الحوار والتفاوض وحل النزاعات، وحماية مصالح وأمن رعايا الدول، حيث أصبح للدبلوماسية الرقمية أهمية متزايدة، مكنت الحكومات من استخدام وسائل التواصل الاجتماعي، والمنصات الرقمية، والذكاء الاصطناعي للتفاعل مع الشعوب، ونقل الرسائل السياسية، وإدارة الأزمات، وحماية البيانات الحساسة، وتعزيز الدبلوماسية الرقمية، وتوسيع نطاق التأثير الدبلوماسي، بشكل أكثر سرعة وفعالية، ومع ذلك، زاد هذا التحول من حدة التحديات التي تواجه التطور الرقمي.

فالحماية الدبلوماسية، التي كانت تقتصر في السابق على حماية الرعايا والشركات في الخارج باستعمال أساليب التفاوض وجهاً لوجه وقنوات الاتصال الدبلوماسية التقليدية، وأحياناً اللجوء إلى القنوات الدولية، تعمل الآن في بيئة رقمية متزايدة حيث تتدفق المعلومات بسرعة عبر الحدود ويمكن أن يتأثر الرأي العام المحلي والدولي على الفور. حيث تتمثل إحدى الفرص الرئيسية التي يوفرها العصر الرقمي في قدرة الدول على التعامل مباشرة مع الجماهير، متجاوزة القنوات الدبلوماسية التقليدية³.

وأصبحت منصات وسائل التواصل الاجتماعي، أدوات قوية للتواصل الدبلوماسي، مما يسمح للمؤسسات وللحكومات بإيصال رسائلها في الوقت الفعلي والمناسب إلى جمهور عالمي. وبالمقابل استقبال الكم الهائل من الرسائل والبيانات، تتيح الدبلوماسية الرقمية أيضاً اتصالات أسرع وأكثر كفاءة بين الدول، مما يعزز سرعة وفعالية المفاوضات وحل النزاعات والمسائل العالقة. وكذلك سهل عملية تواصل الممثلات القنصلية والدبلوماسية مع المواطنين والرعايا بالخارج، وعملية الاشراف وحماية المصالح القومية.

كما أدى التحول الرقمي إلى تطوير أدوات جديدة للدبلوماسية مثل الاجتماعات الافتراضية، والتوقيعات الإلكترونية على الاتفاقيات الدولية، مما جعل العمل الدبلوماسي أكثر كفاءة وأقل تكلفة. في المقابل، أثارت الرقمنة تحديات تتعلق بأمن المعلومات، والتهديدات السيبرانية، والتضليل الإعلامي، مما دفع الدول إلى تبني استراتيجيات لحماية بياناتها وتعزيز أمنها السيبراني كجزء من سياساتها الخارجية.

¹ - Mariana SALAZAR ALBORNOZ, LEGAL NATURE AND LEGAL CONSEQUENCES OF DIPLOMATIC PROTECTION, Mexican Yearbook of International Law, Volume VI, 2006, p 378.

² - Petar Radanliev, Cyber diplomacy: defining the opportunities for cyber security and risks from Artificial Intelligence, JOURNAL OF CYBER SECURITY TECHNOLOGY, Taylor & Francis Group., 2024, pp 01-02

³ . اليونيسكو، التوصيات المتعلقة بأخلاقيات الذكاء الاصطناعي، ص 10، الفقرة 32

وبذلك، أصبح التحول الرقمي عاملاً مزدوج التأثير في العلاقات الدبلوماسية؛ فمن ناحية، عزز القدرة على التفاعل وسرعة التفاوض¹، وأحدث تغييراً جذرياً في كيفية إدارة العلاقات الدبلوماسية بين الدول، وحماية مصالحها ورعاياها في الخارج، ومن ناحية أخرى، فرض تحديات جديدة تتطلب تطوير سياسات دبلوماسية تتماشى مع التطورات التكنولوجية المتسارعة².

وهنا تظهر الحاجة إلى توسيع مفهوم الحماية الدبلوماسية ليشمل البيانات الرقمية، فمع ازدياد اعتماد الدول على البيانات الرقمية في إدارة شؤونها الداخلية والخارجية، أصبحت هذه البيانات عرضة للهجمات السيبرانية والقرصنة³. لذا، برزت الحاجة إلى توسيع نطاق الحماية الدبلوماسية ليشمل تأمين البيانات الرقمية، باعتبارها جزءاً من المصالح الحيوية للدولة ولرعاياها، على حد سواء. ويستلزم ذلك وضع إطار قانوني دولي جديد يُعزز من حماية البيانات الرقمية ويُعالج الجرائم السيبرانية بطريقة فعالة، على غرار تقارير لجنة القانون الدولي المتعلقة بالمسؤولية الدولية، وبالحماية الدبلوماسية.

وفي عصر التحول الرقمي، الذي صارت فيه البيانات الرقمية جزءاً أساسياً من حياة الأفراد والدول والكيانات الاعتبارية⁴، مما يجعل حمايتها قضية ملحة في القانون الدولي. وتقليدياً، تركز الحماية الدبلوماسية على حماية حقوق ومصالح المواطنين والرعايا المادية والقانونية في الخارج⁵، لكن مع تزايد الهجمات السيبرانية، والجرائم الإلكترونية، وانتهاك الخصوصية، وسرقة البيانات الشخصية، يبرز تساؤل حول مدى كفاية هذا المفهوم في ظل التطورات الرقمية.

ومن ثم تتطلب البيئة الرقمية الحديثة إعادة النظر في مفهوم الحماية الدبلوماسية ليشمل الدفاع عن حقوق الأفراد في الفضاء السيبراني، خاصة عند تعرض مواطني دولة معينة لاعتداءات إلكترونية من طرف حكومات أو جهات أجنبية، وما ينجر عن ذلك من خسائر مادية لهؤلاء الأفراد. ويمكن أن يشمل ذلك حالات تسريب البيانات، التجسس الإلكتروني، والاعتداء على الحسابات الرقمية، واختراق قواعد البيانات والمعطيات للأفراد أو الشركات⁶.

وتوسيع نطاق الحماية الدبلوماسية ليشمل البيانات الرقمية يستلزم تطوير أطر قانونية دولية جديدة توازن بين سيادة الدول ومتطلبات حماية الأفراد في العالم الرقمي والافتراضي. كما يتطلب تعزيز التعاون بين الدول لوضع معايير تحكم المسؤولية الدولية عن الهجمات السيبرانية، مما يجعل الحماية الدبلوماسية أكثر شمولاً وملاءمة للتحديات التي يفرضها العصر الرقمي.

المحور الثاني: تحديات التحول الرقمي على المستوى الدولي

¹ . حيدر بدوي صادق، مستقبل الدبلوماسية في ظل الواقع الإعلامي والاتصالي الحديث البعد العربي، دراسات إستراتيجية، ط 1، العدد 05، الإمارات العربية المتحدة: مركز الإمارات للدراسات والبحوث الاستراتيجية، 1996، ص 28 - 29

² - Mary Ellen O'Connell, Cyber Security and International Law, Chatham House, London, 29 may 2012, p 12

³ - Patricio Grané Labat, Naomi Burke, The Protection of Diplomatic Correspondence in the Digital Age: Time to Revise the Vienna Convention, Oxford Academic, England, 2017, pp 204-230

⁴ - Arnaud Tournier, La Protection diplomatique des personnes morales, Paris, LGDJ lextenso, 2013, p 289

⁵ . محمد أمزيان، حماية الدولة لمواطنيها في الخارج عن طريق آلية الحماية الدبلوماسية، مجلة جيل لحقوق الإنسان، العدد 37، ص 121.

⁶ - Joseph Samuel Nye, the future of power, Public Affairs, USA, 2011, pp 113-116

لقد أثر العصر الرقمي بشكل كبير في ممارسة الحماية الدبلوماسية، حيث أدخل فرصاً وتحديات جديدة للعلاقات الدولية. وأدى ظهور تقنيات الاتصالات الرقمية ووسائل التواصل الاجتماعي وتحليلات البيانات المتقدمة إلى إعادة تشكيل كيفية تعامل الدول والمنظمات الدولية والجهات الفاعلة غير الحكومية مع بعضها البعض على المستوى العالمي.

ومع ذلك، فإن العصر الرقمي يقدم أيضاً تحديات كبيرة. تعد تهديدات الأمن السيبراني والمعلومات المضللة وتآكل سيادة الدولة التقليدية في الفضاء الرقمي من الشواغل الأساسية، حيث خلق صعود الدبلوماسية الرقمية طرقاً جديدة للهجمات الإلكترونية وحملات التضليل التي يمكن أن تقوض الجهود الدبلوماسية وتزعزع استقرار الدول والحكومات وحتى العلاقات بين الدول¹. علاوة على ذلك، يمكن أن تؤدي الفجوة التكنولوجية بين الدول المتقدمة والدول النامية إلى اختلالات في الوصول إلى الأدوات الرقمية، مما يؤدي إلى تفاقم عدم المساواة في المشاركة الدبلوماسية العالمية.

ولكون الفضاء السيبراني ميداناً جديداً للصراعات والتحديات الأمنية، ومع التقدم السريع في التكنولوجيا الرقمية، تجاوزت التهديدات الأمنية والجرائم الإلكترونية الحدود التقليدية للدول²، وبدأت تنتشر بوتيرة غير مسبقة، نظراً لارتباطها بالشبكة العالمية للاتصالات. وتشمل هذه التهديدات الهجمات الإلكترونية على البنية التحتية والمعلوماتية للدول، والتجسس الرقمي، وسرقة واختراق البيانات، وشبكات الطاقة والاتصالات والمرافق الحكومية³، وتتسبب في خسائر مادية ومعنوية كبيرة، وهجمات الفدية التي تستهدف الحكومات والشركات والأفراد على حد سواء، وقد تستغلها بعض الكيانات والمنظمات الإجرامية كوسيلة لتهديد الأمن القومي واستقرار الدول.

وتمثل هذه الجرائم تحدياً كبيراً للقوانين الوطنية والدولية، نظراً لطبيعتها العابرة للحدود والتي تجعل من الصعب تحديد الفاعلين أو محاسبتهم قانونياً⁴. على سبيل المثال، قد يُنفَّذ هجوم إلكتروني من دولة معينة ضد أهداف في دولة أخرى دون أن يكون هناك إطار قانوني واضح يسمح بالملاحقة الفعالة للمسؤولين عنه، لتتحول طبيعة الحروب والنزاعات تحولاً جذرياً في العصر الحديث، حيث لم تعد المواجهات مقتصرة على المعارك العسكرية التقليدية فقط⁵، بل أصبحت التكنولوجيا والإعلام أدوات رئيسية في الصراعات الدولية. أدت التطورات التي شهدتها الفضاء السيبراني إلى ظهور الحروب السيبرانية، التي تشمل الهجمات الإلكترونية، والتجسس الرقمي، وسرقة الملكية الفكرية⁶، واختراق الأنظمة الحكومية والمالية وغيرها، مما يجعل الحرب أكثر تعقيداً وخطورة.

¹ - See The Tallinn Manual's Rule 30, North Atlantic Treaty Organization, Tallinn Manual on the International Law applicable to Cyber Warfare, NATO Cooperative Cyber Defence Centre of Excellence, Cambridge University Press, UK, 2013, p. 152

² . منى الأشقر جبور، السيبرانية هاجس العصر، دراسات وأبحاث، المركز العربي للبحوث القانونية والفضائية، بيروت، 2017، ص 41.

³ . محمد أمين الشوبكة، جرائم الحاسوب والانترنت؛ الجريمة المعلوماتية، دار الثقافة للنشر والتوزيع، 2011، الأردن، ص 185 وما بعدها

⁴ - Joseph Samuel Nye, Op.Cit, pp 57-59

⁵ - Alvin Toffler, Powershift, Bantam Books, New York, 1990, p 25

⁶ . منى الأشقر جبور، مرجع سابق، ص 105.

إلى جانب الحرب التكنولوجية، أصبحت الحرب الإعلامية سلاحًا قويًا في التأثير على الرأي العام وتوجيه السياسات، من خلال استخدام وسائل الإعلام التقليدية ومنصات التواصل الاجتماعي لنشر المعلومات المضللة، والدعاية السياسية، والتحكم في السرديات التي تشكل وعي الشعوب. وقد أصبحت الهجمات الإعلامية وحملات التضليل الرقمي جزءًا لا يتجزأ من استراتيجيات الدول والجماعات في تحقيق أهدافها دون اللجوء إلى المواجهات العسكرية المباشرة¹.

هذا التحول في طبيعة الحروب يفرض تحديات جديدة على الأمن القومي والدولي، حيث تحتاج الدول إلى تطوير قدراتها في الأمن السيبراني ومكافحة التضليل الإعلامي، وإلى تكييف قوانينها وتشريعاتها لحماية استقرارها السياسي والاقتصادي، وتنظيم علاقاتها الخارجية بما يخدم مصالحها ومصالح مواطنيها ورعاياها في الخارج².

لمواجهة هذه التحديات، تسعى الدول إلى تعزيز التعاون الدولي عبر اتفاقيات مثل اتفاقية بودابست لمكافحة الجرائم الإلكترونية لعام 2001³، كما تعمل على تطوير سياسات دفاع سيبراني متقدمة لحماية بياناتها ومنظوماتها الرقمية. ومع ذلك، لا تزال هناك حاجة إلى مزيد من التنسيق بين الدول لوضع معايير واضحة تلزم جميع الأطراف بمكافحة الجرائم الإلكترونية العابرة للحدود، وضمان الأمن السيبراني العالمي.

تكمّن خطورة الجرائم الإلكترونية العابرة للحدود في صعوبة تعقب مرتكبيها، نظرًا للطبيعة غير المادية للفضاء السيبراني وإمكانية تنفيذ الهجمات من دول مختلفة دون الحاجة إلى وجود فعلي للمهاجم في الدولة المستهدفة. كما أن غياب إطار قانوني دولي موحد يُعقّد جهود التعاون بين الدول في ملاحقة المجرمين السيبرانيين وتقديمهم للعدالة⁴. وفي حالة الحماية الدبلوماسية فإنه يصعب على الدولة التي يحمل الرعية جنسيتها إثبات أن مواطنها المقيم في دولة أجنبية قد تعرض للضرر بفعل الهجمات السيبرانية، لأن هذا الفعل قد يكون صادرًا من دولة ثالثة وليس من الدول التي يقيم بها الرعية أو بها مصالحه وممتلكاته. إلا إذا تمكنت من إثبات مصدر هذا الفعل.

وكذلك، تعمل الدول والمنظمات الدولية على تطوير سياسات واستراتيجيات لتعزيز الأمن السيبراني، مثل تبادل المعلومات الاستخباراتية، وتوقيع اتفاقيات دولية. ومع ذلك، لا تزال هناك حاجة ملحة لتعزيز التعاون الدولي، ووضع قوانين وبرامج أكثر صرامة لكشف ومحاسبة الجهات الفاعلة في الجرائم الإلكترونية العابرة للحدود، وتعزيز آليات الدفاع الإلكتروني، بهدف تحقيق بيئة رقمية أكثر أمانًا واستقرارًا⁵.

¹ - Alvin Toffler, Op.Cit, p 26

² . محمد محارب، حرب في الفضاء الإلكتروني: اتجاهات وتأثيرات على الكيان الصهيوني، كلية النجاح، نابلس، 2013، ص 86

³ . للإطلاع على نص الاتفاقية، راجع الموقع التالي: <http://www.conventions.coe.int/treaty/EN/treaties/html/185.htm>

⁴ - Tallinn Manual on the International Law applicable to Cyber Warfare, Op.Cit, pp. 96-103

⁵ - Joseph Samuel Nye, Power in the global information age, Routledge, London & NY, 2004, p 201

أما عن تأثير الحماية الدبلوماسية على السيادة الرقمية للدول، في ظل التحول الرقمي المتسارع، لم تعد هذه السيادة تقتصر على الحدود الجغرافية التقليدية، فإضافة إلى كونها لم تعد مطلقة في إطار قواعد حقوق الإنسان¹، فإنها كذلك امتدت إلى الفضاء الإلكتروني والتحكم في التكنولوجيا ووسائل الإعلام، مما يعكس مدى قدرة الدول على حماية بياناتها، وتأمين بنيتها التحتية الرقمية، والسيطرة على تدفق المعلومات داخل أراضيها. حيث أصبحت السيادة الرقمية والتكنولوجية والإعلامية من المفاهيم الحاسمة التي تؤثر على قوة الدول واستقلالها في العصر الحديث. وعلى الرعية الأجنبية احترام سيادة وقوانين الدولة المضيفة²، التي يقيم على أراضيها، وألا يحاول بأي حال من الأحوال اختراق بياناتها أو يكون سبباً في ضرر لهذه الدولة أو لمواطنيها باستعمال الوسائط التكنولوجية، وإلا فلن يستفيد من الحماية الدبلوماسية بسبب عدم توفر شرط نظافة الأيدي. وفي إطارها الرقمي نستخلص ثلاثة أنواع من السيادة:

السيادة الرقمية³ تشير إلى حق الدولة في التحكم في بياناتها الرقمية، وإدارة الإنترنت داخل حدودها، وحماية مواطنيها ورعاياها في الخارج من التهديدات السيبرانية، الداخلية والخارجية، وتعكس هذه السيادة مدى قدرة الدول على تطوير أنظمتها التقنية المستقلة، وتقليل الاعتماد على الشركات والتقنيات الأجنبية، لا سيما في مجالات الأمن السيبراني وتخزين البيانات والذكاء الاصطناعي، وكذا على كفاءة أطرافها ومواطنيها في هذا المجال.

السيادة التكنولوجية وتعني امتلاك الدول للقدرة على تطوير وإنتاج التكنولوجيا المتقدمة محلياً، دون الاعتماد المفرط على القوى التكنولوجية الخارجية الكبرى. ويشمل ذلك تصنيع العدة والعتاد، وتعزيز البحث في مجال الذكاء الاصطناعي والبرمجيات، والقدرة على بناء شبكات اتصالات مستقلة، مثل شبكات الجيل الخامس وتحقيق السيادة التكنولوجية بمنح الدول قوة تنافسية ويقلل من تعرضها للضغوط الاقتصادية أو الأمنية من القوى الأجنبية⁴.

السيادة الإعلامية⁵ وترتبط بقدرة الدولة على التحكم في المحتوى الإعلامي المتداول داخلها، وحماية مجتمعها من المعلومات المضللة والحروب الإعلامية التي قد تستهدف استقرارها الداخلي، وضمان عدم استغلالها لأغراض سياسية أو دعائية من جهات أجنبية. ووضع قوانين لحماية أمن مؤسساتها الإعلامية التقليدية والحديثة، والاستثمار في التكنولوجيا المحلية، وتنظيم المحتوى الإعلامي، مما يضمن لها سيادة قوية في العالم الرقمي الحديث.

¹ . عبد الصمد رحيم كريم زه نكنه، انتهاء مهمة المبعوث الدبلوماسي والبعثة الدبلوماسية، منشورات زين الحقوقية، لبنان، 2016، ص 53.

² . علي خالد الديب، قانون الحماية الدبلوماسية وشروطها، مجلة أهل البيت عليهم السلام، العدد 20، ديسمبر 2016، ص 480.

³ - Gerda Falkner, Digital sovereignty - Rhetoric and reality, Journal of European Public Policy, Vol.31, N° 8, 2024, pp 99-120

See also, Samuele Fratini, Digital Sovereignty: A Descriptive Analysis and a Critical Evaluation of Existing Models, Digital Society, may 2024, pp 59-78

⁴ . محمد مختار، هل يمكن للدول أن تتجنب مخاطر الهجمات الإلكترونية، مجلة اتجاهات الأحداث، العدد 6، مركز المستقبل للأبحاث والتطوير، أبوظبي،

2015، ص 6

⁵ - Monroe E. Price, Media and Sovereignty, The Global Information Revolution and Its Challenge to State Power, The MIT Press, Cambridge, 2004, p 150

أما عن تحديات السيادة الرقمية، فسيادة الدولة في هذا المجال تكمن في مدى قوتها ومدى المامها بمتطلبات العصر، وتكمن أهم هذه التحديات في:

- الاختراقات السيبرانية والتجسس الرقمي الذي يستهدف بيانات الدول ومؤسساتها الحيوية. ورعاياها وشركاتها ومصالحها بالخارج.
- الاحتكار التكنولوجي من قبل شركات ودول تمتلك القوة في مجالات الذكاء الاصطناعي والحوسبة، والضغط لتنظيم استخدام البيانات بشكل يتعارض أحياناً مع المصالح الوطنية.
- الهيمنة الإعلامية والتضليل الرقمي الذي قد يؤثر على استقرار الدول وعلى وعي شعوبها.
- التشابك الاقتصادي العالمي الذي يجعل تحقيق السيادة التكنولوجية¹ الكاملة أمراً معقداً.

هذه المشكلات تزيد من النزاعات والتوترات بين الدول وتدعو إلى ضرورة وضع قواعد دولية لتنظيم السيادة الرقمية للدول²، مع احترام القوانين والمواثيق الدولية المتعلقة بهذا الشأن. ونظراً لقصور القانون الدولي في هذا المجال، بسبب عدم وجود إطار قانوني واضح ينظم اللجوء إلى الحرب الإلكترونية أو يُنظم سير العمليات العدائية خلالها، تم إبرام صك قانوني في عام 2013 يُعرف بـ "تالين". هذا الدليل أعدته مجموعة من خبراء القانون الدولي بدعوة من حلف شمال الأطلسي "الناتو"، بهدف دراسة إمكانية تطبيق قواعد القانون الدولي الإنساني على نزاعات الفضاء السيبراني³.

المحور الثالث: أهمية الحماية الدبلوماسية في مواجهة التحديات الرقمية

في ظل التطورات السريعة في التكنولوجيا والاتصالات الرقمية، أصبح أمن البيانات قضية حيوية تتطلب استراتيجيات متعددة لحمايتها. ومن بين هذه الاستراتيجيات، تلعب الحماية الدبلوماسية دوراً مهماً في تعزيز أمن هذه البيانات على المستوى الدولي. وتتمثل الحماية الدبلوماسية في تدخل الدول لحماية حقوق مواطنيها أو مؤسساتها في الخارج⁴، بما في ذلك البيانات الرقمية والمعلومات الحساسة، والملكية الفكرية والمواقع الإلكترونية، حيث تساهم في بناء جسور التواصل بين الدول لمواجهة التهديدات السيبرانية المشتركة. حيث توفر أساساً قانونياً للمطالبة بحقوق الأفراد والشركات فيما يتعلق بأمن البيانات الرقمية. وهذا يعتبر امتداداً للحماية الدبلوماسية التقليدية، ويمكن أن تساعد في:

¹ - Klaus Illgner, Technological Sovereignty: Methodology and Recommendations, VDE Association, Germany, pp 4-5

² - Tallinn Manual on the International Law applicable to Cyber Warfare, Op.Cit, pp. 15-18

³ . سعيد درويش، ماهية الحرب الإلكترونية في ضوء قواعد القانون الدولي، حوليات الجزائر 1، الجزء الثاني، العدد 29، ص ص 117-137

⁴ . زازة لخضر، مرجع سابق، ص 372

- ضمان التزام الدول المضيفة بحماية البيانات الشخصية للمواطنين الأجانب، ودعم الإطار القانوني لحماية البيانات من خلال المعاهدات الدولية، ووفقاً للاتفاقيات الدولية مثل اللائحة العامة لحماية البيانات (GDPR)¹ في الاتحاد الأوروبي لعام 2016، إضافة إلى تعزيز التعاون مع المنظمات الدولية مثل الإنتربول والأمم المتحدة لمكافحة الجرائم الإلكترونية².
- الضغط على الدول لاحترام معايير الأمن السيبراني وتعزيز التعاون الدولي في هذا مجال، وفرض عقوبات دبلوماسية على الدول أو الجهات التي تنتهك أمن البيانات أو ترعى الهجمات الإلكترونية³.
- استخدام الوسائل الدبلوماسية للتفاوض على اتفاقيات أمن البيانات التي تحدد كيفية تبادل البيانات وحمايتها. وإنشاء قنوات دبلوماسية لحل النزاعات السيبرانية، مما يقلل من مخاطر الهجمات الإلكترونية والتجسس وسرقة البيانات ومنع الأنشطة السيبرانية غير المشروعة، والقرصنة والهجمات الإلكترونية، العابرة للحدود⁴.
- وهنا يبرز دور السفارات والقنصليات في الخارج، حيث تلعب دوراً هاماً في حماية البيانات الخاصة بمواطنيها وشركاتها⁵، من خلال:

- تقديم الدعم القانوني والمشورة للرعايا والشركات بشأن أفضل الممارسات في حماية البيانات أثناء عملها في دول أجنبية.
- العمل على تأمين الخوادم الدبلوماسية والبرمجيات لضمان حماية المعلومات الحساسة المتعلقة بالرعايا وممتلكاتهم وتأمين حساباتهم وكذا الشركات والمصالح الاقتصادية في الخارج⁶.
- تقديم تحذيرات أمنية للمواطنين والرعايا بشأن المخاطر الرقمية المحتملة في البلدان التي يتواجدون بها. إضافة إلى دعم ومساعدة تفعيل أنظمة إلكترونية، تمكن من الإخطار القنصلي المنصوص عنه في المادة 36 من اتفاقية فينا للعلاقات القنصلية 1961.

تلعب الحماية الدبلوماسية دوراً رئيسياً في تعزيز أمن البيانات، سواء من خلال توفير الأطر القانونية، أو عبر الدبلوماسية السيبرانية، أو من خلال تدخل السفارات والقنصليات لحماية مواطنيها⁷. كما أن التعاون الدولي والاتفاقيات القانونية يعدان من أهم الأدوات لضمان حماية البيانات في عالم متصل رقمياً. لذا، فإن تعزيز الدبلوماسية في المجال السيبراني أصبح ضرورة ملحة لمواجهة التهديدات المتزايدة لأمن الرعايا والشركات في الداخل والخارج على حد سواء.

¹ - GDPR General Data Protection Regulation

² . للاطلاع على اللائحة العامة لحماية البيانات الأوروبية راجع الموقع التالي: <https://gdpr-info.eu>

³ - Petar Radanliev, Op.Cit, p06

⁴ . ج. رضوان، الأمن السيبراني، أولوية في استراتيجية الدفاع، مجلة الجيش، مؤسسة المنشورات العسكرية، 630، 2016/1، الجزائر، ص 40

⁵ . سمية رشيد جابر، الحماية الدبلوماسية التي يمارسها القناصل، مجلة المنصور، العدد التاسع، 2006، ص 173.

⁶ - Mariana SALAZAR ALBORNOZ , Op.Cit, p 377.

⁷ . عبد العزيز ناصر عبد الرحمن العبيكان، الحصانات والامتيازات الدبلوماسية والقنصلية في القانون الدولي، ط1، شركة العبيكان للأبحاث والنشر والتطوير، 2007، ص 154.

وفي ظل التوسع الهائل في استخدام الفضاء الرقمي، أصبح تأمين مصالح وحقوق الأفراد والدول، أمرًا بالغ الأهمية. حيث تشمل هذه الحقوق الخصوصية، وحرية التعبير، وحماية البيانات الشخصية¹. وتلعب الحماية الدبلوماسية دورًا محوريًا في تأمين هذه الحقوق من خلال ضمان احترام القوانين الدولية المتعلقة بالإنترنت والعمل على تأمينها وعلى محاسبة الجهات التي تنتهك هذه الحقوق.

وإذا أردنا أن نتحدث على نجاح الحماية الدبلوماسية في حل النزاعات الرقمية المتعلقة بالرعايا والكيانات الاعتبارية في الدول الأجنبية، فلا بد لنا من الإشارة إلى بعض مدى فاعلية بعض الاتفاقيات الدولية التي أبرمت لمكافحة الجريمة السيبرانية، مثل "اتفاقية بودابست" سالفة الذكر². كما ساهمت الجهود الدبلوماسية في تهدئة التوترات بين الدول الناتجة عن اتهامات بالتجسس الرقمي وسرقة البيانات، من خلال آليات الحوار والتفاوض باعتباره وظيفة من الوظائف الدبلوماسية.

وكذلك مبادئ منظمة التعاون والتنمية الاقتصادية (OECD)³ بشأن الأمن الرقمي والذكاء الاصطناعي لعام 2019، التي تم تبنيها من قبل 42 دولة، بما في ذلك الولايات المتحدة ودول الاتحاد الأوروبي، تدعو إلى تطوير أنظمة وبرامج ذكاء اصطناعي موثوقة ومسؤولة، مع احترام حقوق الإنسان وخصوصية الأشخاص الطبيعية والاعتبارية. إضافة إلى جهود الأمم المتحدة والهيئات التابعة لها في هذا المجال. حيث اعتمدت الجمعية العامة للأمم المتحدة يوم 24 ديسمبر 2024، اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية، وهي اتفاقية عالمية تاريخية تهدف إلى تعزيز التعاون الدولي لمكافحة الجريمة السيبرانية وحماية المجتمعات من التهديدات الرقمية⁴.

المحور الرابع: مستقبل الحماية الدبلوماسية في عصر الرقمنة

تبرز أهمية تطوير القوانين الدولية والداخلية لمواكبة التحديات الرقمية، مع استمرار تطور التكنولوجيات الرقمية وظهور تهديدات جديدة، أصبح من الضروري تحديث القوانين الدولية والداخلية لتشمل حماية البيانات السيبرانية والأمن الرقمي. يهدف ذلك إلى سد الفجوات القانونية وتنظيم المسؤولية الدولية تجاه الجرائم الإلكترونية، مما يعزز من استقرار العلاقات بين الدول في الفضاء الرقمي⁵.

¹ . اليونسكو، مرجع سابق، ص 5، الفقرة ج

² . وليد طه، التنظيم التشريعي للجرائم الإلكترونية في اتفاقية بودابست، قطاع التشريع بوزارة العدل، مصر، بدون سنة طبع، ص 23-25

³ - OECD L'Organisation de coopération et de développement économiques
<https://www.state.gov/the-organization-for-economic-co-operation-and-development-oecd>

⁴ . الجمعية العامة للأمم المتحدة، الدورة التاسعة والسبعون، اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية، ديسمبر 2024، الوثيقة A/RES/79/243

⁵ - Petar Radanliev, Op.Cit, pp 04-05

وتجسد ذلك من خلال عدة اتفاقيات دولية، مثل اتفاقية الأمم المتحدة بشأن مكافحة الجريمة المنظمة عبر الوطنية¹ (UNTOC) لعام 2000، وتتعلق بالجرائم المنظمة العابرة للحدود، بما في ذلك الجرائم السيبرانية، القرصنة والاستغلال غير المشروع للتكنولوجيا. وتهدف الاتفاقية إلى تعزيز التعاون الدولي في مجال مكافحة الجريمة المنظمة، بما في ذلك الجرائم التي تُرتكب باستخدام الإنترنت والتكنولوجيات الحديثة. تتضمن بنودًا تتعلق بتبادل المعلومات، وتحقيق العدالة في حالات الجرائم العابرة للحدود.

كما أن التعاون الدولي لتعزيز الحماية الدبلوماسية في المجال السيبراني يمثل ركيزة أساسية للتصدي للتحديات العابرة للحدود في هذا المجال. يتضمن ذلك تبادل المعلومات والخبرات بين الدول²، والتفاوض على اتفاقيات سيبرانية جديدة، وإنشاء آليات مشتركة لمراقبة الفضاء الرقمي وحمايته. هذا النوع من التعاون يعزز من قدرة الدول على مواجهة التهديدات الرقمية بشكل جماعي وفعال. وتجسيدا لذلك جاءت عدة اتفاقيات، منها اتفاقية حماية البيانات الشخصية في أمريكا اللاتينية (AHCET)³، وهي اتفاقية إقليمية بين دول أمريكا اللاتينية لمواكبة التطورات العالمية في حماية البيانات الشخصية للأفراد والكيانات الاعتبارية الأخرى، بما فيهم الرعايا الأجانب. وتركز هذه الاتفاقية على تحقيق توازن بين حماية الخصوصية وحرية التجارة الرقمية، وحماية ممتلكات ومصالح الرعايا الأجانب من الاختراق والقرصنة، وتوفير أسسًا قانونيًا لتقوية حماية البيانات الشخصية على المستوى الإقليمي.

واستخدام التكنولوجيا المتقدمة، مثل الذكاء الاصطناعي، لتعزيز الأمن الدبلوماسي، حيث تلعب التكنولوجيا المتقدمة، وخاصة الذكاء الاصطناعي، دورًا متزايد الأهمية في تعزيز الأمن الدبلوماسي. ويمكن استخدامه من تحليل البيانات الضخمة⁴، واكتشاف التهديدات السيبرانية بسرعة، وتقديم حلول استباقية لحماية الأنظمة الرقمية، كما يتيح الذكاء الاصطناعي تحسين عمليات اتخاذ القرار في المجال الدبلوماسي من خلال تقديم رؤى دقيقة حول التهديدات الرقمية.

ومن ذلك نجد، إعلان اليونسكو بشأن أخلاقيات الذكاء الاصطناعي لعام 2021، يركز على تطوير واستخدام الذكاء الاصطناعي بطريقة تحترم حقوق الإنسان وتعزز التنمية المستدامة. ويشدد على أهمية الشفافية، والمساءلة القانونية والاستغلال الإيجابي لأنظمة الذكاء الاصطناعي⁵.

¹ - UNTOC The United Nations Convention against Transnational Organized Crime
<https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html>

² . مصطفى بخوش، "مستقبل الدبلوماسية في ظل التحولات الدولية الراهنة"، مجلة المفكر، العدد الثالث، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، الجزائر، ص 93 - 94

³ - AHCET Asociación Hispanoamericana de Centros de Investigación y Empresas de Telecomunicaciones

⁴ . أنظر: ديفيد أوماند وآخرون، استخبارات وسائل التواصل الاجتماعي، تر: مركز الامارات للبحوث والدراسات الاستراتيجية، ط 1، سلسلة دراسات عالمية، الإمارات العربية المتحدة: مركز الامارات للبحوث والدراسات الاستراتيجية، العدد 125، 2014، ص 16 - 23

⁵ . اليونسكو، مرجع سابق، ص 10، الفقرة 31

وهناك جهود متزايدة لإبرام اتفاقيات دولية ملزمة قانونيًا، خصوصًا مع تصاعد تأثير الذكاء الاصطناعي على الأمن، الاقتصاد، وحقوق الإنسان، نتيجة سوء استغلاله، حيث قامت الدول والمؤسسات الكبرى بالسعي لوضع سياسات متوازنة تحقق الفوائد دون الإضرار بالأفراد والمجتمعات، وبالرعايا الطبيعيين والاعتباريين¹ مهما كانت انتماءاتهم، كما تمكنت من اقناع المجتمع الدولي بتبني "الميثاق العالمي للأمم المتحدة حول الذكاء الاصطناعي"، في قمة المستقبل شهر سبتمبر 2024² ويهدف إلى وضع معايير دولية واضحة لتنظيم استغلال الفضاء الافتراضي والذكاء الاصطناعي بما يخدم البشرية ويقلل من المخاطر المترتبة عن سوء استخدام البرامج والوسائط التكنولوجية. وذلك وفق ضوابط أخلاقية، وضمان تسخيرها لبناء عالم أكثر شمولاً واستدامةً وسلاماً³.

وكذلك الإطار التنظيمي للاتحاد الأوروبي للذكاء الاصطناعي، الذي اقترحتة المفوضية الأوروبية عام 2021 ليكون أول قانون شامل ينظم الفضاء السيبراني والذكاء الاصطناعي عالميًا. ويصنف أنظمة الذكاء الاصطناعي والبرامج الإلكترونية حسب مستوى المخاطر (من منخفضة إلى عالية) ويفرض قيودًا صارمة على التطبيقات عالية المخاطر، ويحدد المسؤوليات للمشرفين عنها، كما يمنع بعض الاستخدامات مثل التعرف التلقائي على الوجه في الأماكن العامة.

أما عن الاتجاهات المستقبلية للحماية الدبلوماسية، فقد صارت تواجه تحديات جديدة تتطلب تحولاً جذرياً في أساليبها التقليدية. فمن المتوقع أن يشهد المستقبل تعزيز الأمن السيبراني في السفارات والبعثات الدبلوماسية عبر أنظمة متقدمة لحماية البيانات والاتصالات الرسمية من الهجمات الإلكترونية، إلى جانب تبني الدبلوماسية الرقمية التي تعتمد على الذكاء الاصطناعي وتحليل البيانات لاتخاذ قرارات مبنية على معلومات دقيقة وسريعة، بالإضافة إلى استخدام تقنيات مثل البلوك تشين لتأمين الوثائق والمراسلات⁴.

وبذلك، ستعتمد الحماية الدبلوماسية في المستقبل على استراتيجيات متقدمة تجمع بين التكنولوجيا الحديثة، والأمن السيبراني، والتعاون الدولي لضمان أمن الدول ومصالحها الدبلوماسية في الخارج وفي الفضاء الرقمي⁵. فيما سيتم فرض تدابير أمنية مشددة لحماية الحسابات الرسمية للدبلوماسيين من الاختراق وتقديم تدريبات إلزامية لهم حول الأمن السيبراني. إضافة إلى ذلك، ستتجه الدول إلى مكافحة التضليل الإعلامي والدبلوماسية الزائفة عبر آليات تحقيق متطورة، مع تعزيز التعاون مع شركات التكنولوجيا الكبرى لمواجهة الأخبار المزيفة والتدخلات الرقمية.

¹ - Arnaud Tournier, Op.Cit, p 87

² - الاطلاع على الميثاق والوثائق المرافقة المتعلقة به عبر الموقع : <https://www.un.org/ar/summit-of-the-future>

³ - David Wicki-Birchler, The Budapest Convention and the General Data Protection Regulation: acting in concert to curb cybercrime, Int. Cybersecur. Law Rev. 2020, p 65.

⁴ - Petar Radanliev, Op.Cit, p 07 , See also Suhag A & Daniel DA. Study of statistical techniques and artificial intelligence methods in distributed denial of service (DDOS) assault and defense. Journal of Cyber Security technology, Volume 07, Issue 1, 2023, pp 21–51

⁵ - Petar Radanliev, Ibid, p 06

وحسب رأينا فإن المشكلة تكمن في أهمية العلاقة بين التغيير التكنولوجي المتسارع، والسياق المجتمعي الأوسع الذي يحدث فيه، محلياً ودولياً، ومدى تقبل المجتمع لعملية التغيير، وهي وجهة نظر يؤكدتها منظور تاريخي للحماية الدبلوماسية، ولكون التطور عملية ديناميكية تتأثر بالمتغيرات الدولية. فإننا نتوقع أن صيغة العلاقات الدولية والحماية الدبلوماسية الراهنة، يمكن أن تختلف عن تلك التي سنجدها في المستقبل، جنباً إلى جنب مع التغيرات الاجتماعية والسياسية والاقتصادية... وعلاوة على ذلك، فإن بعض الدول عدلت قوانينها وتشريعاتها على ضوء البيئة الدولية المتغيرة التي ساعدت في تهيئة ظروف محلية محددة، غلب عليها الطابع الرقمي بما يحمله من فوائد وانتكاسات.

الخاتمة

وفي عصر التحول الرقمي، أصبحت حماية البيانات والخصوصية قضية عالمية تتطلب تعاوناً دولياً وأدوات دبلوماسية فعالة. حيث يمكن للحماية الدبلوماسية أن تلعب دوراً رئيسياً في نقطتين أساسيتين:

- التفاوض على اتفاقيات دولية تعزز حماية البيانات، والدعوة إلى تعزيز الدراسات والأبحاث حول هذا الموضوع لضمان حماية المصالح العالمية. حيث من خلال تعزيز الحماية الدبلوماسية في هذا المجال، يمكن للدول أن تضمن بيئة رقمية آمنة لمواطنيها وشركاتها في الخارج في عالم يتسم بالتراطيب الرقمي المتزايد. وضرورة التدخل لحماية حقوق الأفراد والشركات في حالات انتهاك الخصوصية¹.

- تعزيز التعاون بين الدول لمواجهة التهديدات الإلكترونية، والتأكيد على الحاجة إلى هذا التعاون لمواجهة التحديات المستقبلية. لكون الحماية الدبلوماسية في عصر التحول الرقمي، تتجاوز المفاهيم التقليدية لتشمل قضايا مثل الأمن السيبراني وحماية البيانات وحقوق الإنسان الرقمية². وأصبحت هذه الحماية ضرورية لمواجهة التحديات الجديدة التي تفرضها البيئة الرقمية، مما يتطلب تطوير أدوات دبلوماسية حديثة لضمان حماية مصالح وخصوصية وأمن الأفراد والدول في العصر الرقمي المتطور.

وبالرجوع إلى الوظائف التقليدية للدبلوماسية، المتمثلة أساساً في حماية المصلحة القومية للبلاد، ومنها حماية الرعايا والممتلكات والمصالح الاقتصادية، الثقافية، العسكرية، والسياسية... نجد، أن طبيعة هذه الوظائف قد تغيرت أساليبها، تماشياً مع متطلبات ومتغيرات العصر الرقمي، لتتكيف مع الأوضاع الدولية الراهنة (وظيفة التمثيل، وظيفة الاستعلام، وظيفة التفاوض)

إضافة إلى ذلك فإن حماية حقوق الإنسان الرقمية قد أصبحت ضرورة ملحة لا يمكن تجاهلها. فمع انتشار الإنترنت وزيادة الاعتماد على التقنيات الحديثة في مختلف جوانب الحياة، ازدادت التهديدات التي تتعلق بخصوصية الأفراد وحررياتهم. وتُعد

¹ . اليونيسكو، مرجع سابق، ص 17، فقرة 72

² . اليونيسكو، نفس المرجع، ص 16، الفقرة 61

حقوق الإنسان الرقمية امتدادًا لحقوق الإنسان الأساسية، حيث تشمل الحق في الخصوصية، وحرية التعبير، والحماية من المراقبة غير المشروعة، والوصول العادل إلى المعلومات. ومع تطور تقنيات الذكاء الاصطناعي وتحليل البيانات، أصبحت هناك حاجة ماسة لتشريعات وقوانين تضمن حماية هذه الحقوق من الاستغلال أو الانتهاك. كما أن التطور التكنولوجي، رغم فوائده الكبيرة، يحمل في طياته مخاطر مثل اختراق البيانات والتلاعب بالمعلومات، مما يتطلب تعاونًا دوليًا لضمان أن تكون التكنولوجيا أداة لتعزيز حقوق الإنسان وليس وسيلة لقمعها. لذا، يجب أن تسير حماية الحقوق الرقمية جنبًا إلى جنب مع التقدم التكنولوجي، لضمان عالم رقمي آمن وعادل للجميع.

وفي ختام هذا الموضوع، يتضح أن حماية الأفراد والدول في العصر الرقمي لم تعد خيارًا، بل ضرورة حتمية تتطلب الوعي والتخطيط والاستثمار في الأمن السيبراني. فمع تزايد التهديدات الإلكترونية وتعقيدها، يجب أن تتكاتف الجهود بين الحكومات، والمؤسسات، والأفراد لضمان بيئة رقمية آمنة تحمي البيانات والخصوصية وتحافظ على الاستقرار. كما أن تعزيز الثقافة الأمنية¹، والالتزام بالتشريعات، وتطوير التقنيات الحديثة، كلها عوامل أساسية في بناء مستقبل رقمي أكثر أمانًا واستدامة. وبالتالي تحقيق الهدف الأسمى الذي بني عليه ميثاق الأمم المتحدة، وهو حفظ السلم والأمن الدوليين.

المراجع

1. زارة لخضر، أحكام المسؤولية الدولية في ضوء قواعد القانون الدولي العام، دار الهدى للطباعة والنشر والتوزيع، الجزائر، 2011.
2. فوزي أوصديق، مبدأ التدخل والسيادة لماذا؟ وكيف؟، دار الكتاب الحديث، الجزائر، 1999.

¹ . الجمعية العامة للأمم المتحدة، الدورة التاسعة والسبعون، مكافحة استعمال تكنولوجيا المعلومات والاتصالات لأغراض إجرامية، نوفمبر 2024،

3. الأمم المتحدة، المفوضية السامية لحقوق الإنسان، العهد الدولي الخاص بالحقوق المدنية والسياسية
4. محمد أمزيان، حماية الدولة لمواطنيها في الخارج عن طريق آلية الحماية الدبلوماسية، مجلة جيل لحقوق الإنسان، العدد 37
5. منى الأشقر جبور، السيبرانية هاجس العصر، دراسات وأبحاث، المركز العربي للبحوث القانونية والقضائية، بيروت، 2017
6. محمد أمين الشوبكة، جرائم الحاسوب والانترنت؛ الجريمة المعلوماتية، دار الثقافة للنشر والتوزيع، 2011، الأردن
7. محمد محارب، حرب في الفضاء الإلكتروني: اتجاهات وتأثيرات على الكيان الصهيوني، كلية النجاح، نابلس، 2013
8. عبد الصمد رحيم كريم زه نكنه، انتهاء مهمة المبعوث الدبلوماسي والبعثة الدبلوماسية، منشورات زين الحقوقية، لبنان، 2016
9. علي خالد الديس، قانون الحماية الدبلوماسية وشروطها، مجلة أهل البيت عليهم السلام، العدد 20، 2016
10. محمد مختار، هل يمكن للدول أن تتجنب مخاطر الهجمات الإلكترونية، مجلة اتجاهات الأحداث، العدد 6، مركز المستقبل للأبحاث والتطوير، أبوظبي، 2015
11. سعيد درويش، ماهية الحرب الإلكترونية في ضوء قواعد القانون الدولي، حوليات الجزائر 1، الجزء الثاني، العدد 29
12. ج. رضوان، الأمن السيبراني، أولوية في استراتيجية الدفاع، مجلة الجيش، مؤسسة المنشورات العسكرية، 630، 2016/1، الجزائر
13. سمية رشيد جابر، الحماية الدبلوماسية التي يمارسها القناصل، مجلة المنصور، العدد التاسع، 2006
14. وليد طه، التنظيم التشريعي للجرائم الإلكترونية في اتفاقية بودابست، قطاع التشريع بوزارة العدل، مصر، ب ط
15. عبد العزيز ناصر عبد الرحمن العبيكان، الحصانات والامتيازات الدبلوماسية والقنصلية في القانون الدولي، ط1، شركة العبيكان للأبحاث والنشر والتطوير، 2007
16. حيدر بدوي صادق، مستقبل الدبلوماسية في ظل الواقع الإعلامي والاتصالي الحديث البعد العربي، دراسات إستراتيجية، ط 1، العدد 05، الإمارات العربية المتحدة: مركز الإمارات للدراسات والبحوث الاستراتيجية، 1996
17. ديفيد أوماند وآخرون، استخبارات وسائل التواصل الاجتماعي، تر: مركز الامارات للبحوث والدراسات الاستراتيجية، ط 1، سلسلة دراسات عالمية، الإمارات العربية المتحدة: مركز الامارات للبحوث والدراسات الاستراتيجية، العدد 125، 2014
18. مصطفى بخوش، مستقبل الدبلوماسية في ظل التحولات الدولية الراهنة، مجلة المفكر، العدد الثالث، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، الجزائر
19. اتفاقية بودابست لمكافحة الجرائم الإلكترونية، على الموقع: (07 ديسمبر 2024، 23.00)
<http://www.conventions.coe.int/treaty/EN/treaties/html/185.htm>
20. اللائحة العامة لحماية البيانات الأوروبية، على الموقع (08 ديسمبر 2024، 00:30)
<https://gdpr-info.eu>

21. اعلان اليونسكو بشأن اخلاقيات الذكاء الاصطناعي، (10 ديسمبر 2024، 10:45)
https://unesdoc.unesco.org/ark:/48223/pf0000380455_ara
22. الجمعية العامة للأمم المتحدة، الدورة التاسعة والسبعون، مكافحة استعمال تكنولوجيا المعلومات والاتصالات لأغراض إجرامية، نوفمبر 2024، الوثيقة A/79/460، (25 جانفي 2025، 01:20)
<https://docs.un.org/ar/A/79/460>
23. الجمعية العامة للأمم المتحدة، الدورة التاسعة والسبعون، اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية، ديسمبر 2024، الوثيقة A/RES/79/243، (25 جانفي 2025، 02:30)
<https://docs.un.org/ar/A/RES/79/243>
24. ميثاق الأمم المتحدة حول الذكاء الاصطناعي، قمة المستقبل 2024،
<https://www.un.org/ar/summit-of-the-future>
25. Mariana Salazar Alborno, **Legal Nature and Legal Consequences of Diplomatic Protection**, Mexican Yearbook of International Law, Volume VI, 2006.
26. Arnaud Tournier, **La Protection diplomatique des personnes morales**, Paris, LGDJ lextenso, 2013
27. Joseph Samuel Nye, **The Futur of Power**, Public Affairs, USA, 2011
28. **The Tallinn Manual**, North Atlantic Treaty Organization, Tallinn Manual on the International Law applicable to Cyber Warfare, NATO Cooperative Cyber Defence Centre of Excellence, Cambridge University Press, UK, 2013
29. Alvin Toffler, **Powershift**, Bantam Books, New York, 1990
30. Gerda Falkner, **Digital sovereignty - Rhetoric and reality**, Journal of European Public Policy, Vol.31, N° 8, 2024
31. Samuele Fratini, **Digital Sovereignty: A Descriptive Analysis and a Critical Evaluation of Existing Models**, Digital Society, may 2024
32. David Wicki-Birchler, **The Budapest Convention and the General Data Protection Regulation: acting in concert to curb cybercrime?** Int. Cybersecur. Law Rev. 2020
33. Joseph Samuel Nye, **Power in the global information age**, Routledge, London & NY, 2004
34. Patricio Grané Labat, Naomi Burke, **The Protection of Diplomatic Correspondence in the Digital Age : Time to Revise the Vienna Convention**, Oxford Academic, England, 2017
35. Mary Ellen O'Connell, **Cyber Security and International Law**, Chatham House, London, 29 may 2012
36. Petar Radanliev, **Cyber diplomacy: defining the opportunities for cybersecurity and risks from Artificial Intelligence**, JOURNAL OF CYBER SECURITY TECHNOLOGY, Oxford University, February 2024
37. Suhag A & Daniel DA. **Study of statistical techniques and artificial intelligence methods in distributed denial of service (DDOS) assault and defense**. Journal of Cyber Security technology, Volume 07, Issue 1, 2023
38. Monroe E. Price, **Media and Sovereignty, The Global Information Revolution and Its Challenge to State Power**, The MIT Press, Cambridge, 2004, p 150

39. Klaus Illgner, **Technological Sovereignty: Methodology and Recommendations**, VDE Association, Germany, pp 4-5
40. OECD **L'Organisation de coopération et de développement économiques** (Consulted on 07 December 2024 at 23.30), <https://www.state.gov/the-organization-for-economic-co-operation-and-development-oecd>
41. UNTOC **The United Nations Convention against Transnational Organized Crime** (Consulted on 01 December 2024 at 23.30) <https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html>
42. AHCIET **Asociación Hispanoamericana de Centros de Investigación y Empresas de Telecomunicaciones** (Consulted on 23 December 2024 at 20:30) <https://telos.fundaciontelefonica.com/archivo/numero057/ahciet-2/>