

استراتيجيات تعزيز المواطنة الرقمية والأمن السيبراني في ظل البيئة الرقمية: مقاربة نظرية

Strategies for Promoting Digital Citizenship and Cybersecurity in the Digital Environment: A Theoretical Approach

حميدة موافي بناني¹ * الحسين شربالي²

¹ جامعة محمد خيضر، بسكرة، الجزائر hamida.mouakibanani@univ-biskra.dz

² جامعة عمار ثلجي الأغواط، الجزائر ho.cherbali@lagh-univ.dz

تاريخ الإرسال: 2025/05/26 تاريخ القبول: 2025/06/22 تاريخ النشر: 2025/06/30

الملخص:

أصبح مفهوم المواطنة الرقمية حقيقة في ظل ولادة مجتمع المعلومات وتطور تكنولوجيا الاتصال الحديثة وامتداد نسيجها الشبكاتي على مساحة واسعة من النشاط الإنساني، أدى هذا إلى ظهور مقترَب مفاهيمي جديد و موازي له ، الذي يتمثل في الأمن السيبراني وهو يعد بمثابة تحدي يجب تحقيقه بعد تلاحم أدوات الاتصال مع الأدوات المحوسبة لتنتج مناخا من نمط جديد امتزجت فيه البيئة التواصلية بالمؤثرات الصوتية والمرئية فحدث هذا التحول الجديد ، الذي أدى الى خلق بيئة اجتماعية افتراضية رقمية ، أو ما يصطلح على تسميته " المواطنة الرقمية" ولن يتحقق هذا المعطى إلا في ظل توفر أمن معلوماتي يحمي بيانات هؤلاء المواطنين الرقميين ، سواء كانوا افراد أو جماعات. سنحاول في هذه الورقة البحثية مطارحة مفهوم الأمن السيبراني و دوره في تعزيز المواطنة الرقمية، من خلال رصد أهم الاستراتيجيات المتبعة في ذلك ، ومدى إمكانيات تحقيقها .

الكلمات المفتاحية: المواطنة الرقمية، الأمن السيبراني، تكنولوجيا الاتصال الحديثة، البيئة

الرقمية.

Abstract:

The concept of digital citizenship has become a tangible reality with the emergence of the information society and the advancement of modern communication technologies, whose networked structures have extended across vast domains of human activity. This evolution has given rise to a new and parallel conceptual approach—namely, cybersecurity—which represents a critical challenge to be addressed. The convergence of communication tools with computerized systems has produced a new kind of environment in which communicative settings are fused with audiovisual influences, leading to a transformative shift that has created a digital, virtual social space—commonly referred to as "digital citizenship." This notion, however, cannot be fully realized without the presence of robust information security that safeguards the data of these digital citizens, whether individuals or groups. In this research paper, we aim to examine the concept of cybersecurity and its role in strengthening digital citizenship by analyzing the key strategies adopted in this context and evaluating the extent to which they can be effectively implemented.

Keywords: Digital Citizenship, Cybersecurity, Modern Communication Technologie, Digital Environment.

مقدمة:

في خضم التغيرات الرقمية المتسارعة، واعتماد الأفراد والمؤسسات على التكنولوجيات الحديثة في مختلف الأصعدة، تزايدت التهديدات الرقمية وسرقة البيانات وانتهاك الخصوصية، مما جعل الأمن الرقمي حتمية، لا مجرد خيار تقني. ويعد الأمن السيبراني بتجلياته المتنوعة كالأمن السيبراني، الأمن المعلوماتي والأمن الإلكتروني أحد التحديات الحالية والمستقبلية التي تواجهها المؤسسات الحكومية والخاصة لتحقيقه بشكل فعال.

وفي علاقة ارتباطية تكاملية لتجسيد الاستخدام الآمن للتكنولوجيا، استلزم على الأفراد و المؤسسات والحكومات اتخاذ إجراءات وسياسات فعالة لحماية البيانات والمعلومات الحساسة،

وتوفير البرامج والأدوات الضرورية لتحقيق الأمن الرقمي، بما في ذلك استخدام تقنيات التشفير والوصول المحدد والمصادقة المتعددة العوامل والتدابير الأمنية الأخرى، بالإضافة إلى ضرورة اكتساب الوعي السيبراني للأفراد و إتباع ممارسات الأمان الرقمي، وهذا ما يتضمنه مفهوم المواطنة الرقمية.

على ضوء هذه المطارحات القائمة يجوز لنا طرح الاشكال التالي :

التساؤل الرئيسي:

- ما هي أهم الاستراتيجيات المتبعة لتحقيق الأمن السيبراني داخل البيئة الرقمية الجديدة من أجل تعزيز فعالية المواطنة الرقمية ؟

التساؤلات الفرعية:

1. فيما تتمثل أبرز استراتيجيات تعزيز المواطنة الرقمية من منظور الأمن السيبراني في ظل البيئة الرقمية؟
2. فيما تتمثل مساهمات المجتمع الدولي لإرساء المواطنة الرقمية الفعالة في ظل الأمن السيبراني؟

أولاً: تحديد المفاهيم:

عادة ما ينظر إلى أي طرح من خلال المفاهيم التي يتركز عليها، لفهم ما يمكن أن يعالجه هذا المنظور، لذا كان لازماً على أي دراسة تحديد الزوايا المقصودة في المفاهيم المستخدمة.

1. الأمن السيبراني:

أ. لغة:

تعتبر كلمة سيبرانية أو ساير أو سيبراني ترجمة حرفية لكلمة **Cyber** والمشتقة من كلمة **Cyberntics**. وقد استخدم هذا المصطلح أكاديمياً **Cyberntics** من قبل عالم الرياضيات

الأمريكي norbert wieners 1948، في كتابه الشهير: علم التحكم الآلية أو التحكم والاتصال في الحيوان والآلة وذلك للإشارة إلى آليات التنظيم الذاتي.¹

قاموس مصطلحات الأمن المعلوماتي: السيبرانية هو: هجوم عبر الفضاء الإلكتروني يهدف إلى السيطرة على مواقع الإلكترونية أو بنى محمية الكترونيا لتعطيلها أو تدميرها أو الاضرار بها.²

وفي اللغة العربية حسب ما يجمع عليه الباحثين المتخصصين أنه لا يوجد مصطلح يناظر كلمة "ساير" ومرجع ذلك الى أن هذا العلم حديث النشأة لم يظهر في الوطن العربي في وقت سابق ، وإنما ظهر في الغرب.³

ب. اصطلاحا:

عرفه الباحثان Neittaanmaki pekka ;lehto Martti في كتابهما: cyber security: "هو تلك الحزمة من الإجراءات التي تتخذ في الدفاع ضد هجمات قرصنة الكمبيوتر وعواقبها وذلك بإتخاذ كل التدابير المضادة التي تتطلب ذلك".⁴

عرفه ادوارد أمورسو بأنه: "وسائل من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات، وتشمل تلك الوسائل الأدوات المستخدمة في مواجهة القرصنة وكشف الفيروسات ووقفها، وتوفير الاتصالات المشفرة".⁵

يعرف الأمن السيبراني على النحو المحدد في توصية الاتحاد الدولي للاتصالات بأنه: مجموعة الأدوات والسياسات والمفاهيم الأمنية والضمانات الأمنية والمبادئ التوجيهية وثهج إدارة المخاطر والإجراءات والتدريب وأفضل الممارسات وسبل الضمان والتكنولوجيات التي يمكن استخدامها في حماية البيئة السيبرانية والمنظمة وأصول المستعملي. وتشمل المنظمة وأصول المستعملي تجهيزات الحواسيب الموصولة، والموظفي، والبنية التحتية، والتطبيقات، والخدمات، وأنظمة الاتصالات، والحصيلة الكلية للمعلومات المرسله و/أو المخزنة في البيئة السيبرانية. ومن شأن خدمات الأمن

السيبراني كفالة التحقيق والحفاظ على الخواص الأمنية للمنظمات وأصول المستعملي إزاء المخاطر الأمنية ذات الصلة في البيئة السيبرانية.⁶

ج. اجرائيا: مجموعة الإجراءات والتقنيات والممارسات التي تهدف الى حماية البيانات وخصوصية الأفراد من الهجمات الالكترونية أو الوصول غير المصرح به أو السرقة... الخ .

2. مجتمع المعلومات :

أ. اصطلاحا:

يعتبر مصطلح "مجتمع المعلومات من المصطلحات الحديثة التي ظهرت في النصف الثاني من القرن العشرين، فكان بمثابة الحقيقة الواقعية التي بدأت بعض الدول معاشتها وتطمح دول أخرى الى بلوغها، فالضبط المفاهيمي لهذا المصطلح لا يزال غير متحكم فيه وغير واضح المعالم، فنوجز بعض التعاريف التي صيغت من طرف بعض الأكاديميين و الباحثين التي حاولت ضبط مفهوم هذا المصطلح نذكر منها :

هو مجتمع تتاح فيه الاتصالات العالمية وتنتج فيه المعلومات بكميات ضخمة، كما توزع توزيعا واسعا، والتي تصبح فيه المعلومات لها تأثير على الاقتصاد.⁷

كما ورد في التقرير العالمي لليونيسكو 2005 " من مجتمع المعلومات إلى مجتمع المعرفة " حيث وصف مجتمع المعرفة بالمجتمع الذي لديه القدرة على تحديد و إنتاج و معالجة وتحويل و نشر واستعمال المعرفة من أجل التنمية الانسانية ، كما يردف التقرير من أن مجتمعات المعلومات تستند على الحريات الأساسية وبخاصة حرية التعبير وتسمح في رؤيتها بتطبيق أفضل لحقوق الانسان العالمية، الاستقلالية، التعددية، الانخراط و المشاركة و محاربة الفقر و أن المعرفة تعد بمثابة أداة لاشباع الحاجات الاقتصادية و مكون أساسي وفعال لتحقيق التنمية الشاملة.⁸

كما عرفه "عبد الهادي محمد فتحي": بأنه هو المجتمع الذي يعتمد على المعلومة الوفيرة كمورد استثماري، كسلعة استراتيجي ، كخدمة ، كمصدر للدخل القومي و كمجال للقوة العامة .⁹ تت

1. اجرائيا: هو المجتمع الذي يعتمد على المعلومات وتكنولوجيات الاتصال في جميع مجالاته: التعليم، الإعلام، الإقتصاد... الخ.

3. تكنولوجيا الاتصال الحديثة :

أ. اصطلاحا:

يقصد بها المعرفة المنهجية للتقنية، فهي مجموع المعارف العلمية والتقنية التي يجب أن نتحكم من أجل تشكيل الأهداف بالتكنولوجيات تتطور وفق العلوم والتقنيات فهما متلازمتين وتنشر بفعل انساق السريان العادي أو التقليد.¹⁰

وتعرف أيضا بأنها مجموعة الأدوات والأجهزة التي توفر عملية تخزين المعلومات ومعالجتها، ومن ثم إسترجاعها وتوصيلها بعد ذلك إلى أجهزة الاتصالات المختلفة إلى أي مكان في العالم، فهي تغطي أي منتج يقوم بتخزين، واسترجاع ومعالجة وإرسال أو تلقي المعلومات إلكترونيا بشكل رقمي.¹¹

ب. اجرائيا: الوسائل الرقمية التي تستخدم لنقل المعلومات وتبادلها بسرعة وفعالية بين الأفراد: كالهواتف الذكية، الحواسيب، البريد الإلكتروني، تطبيقات التواصل الاجتماعي.

4. المواطنة الرقمية :

أ. اصطلاحا:

من الاعتقادات السائدة لدى الكثيرين هو أن المواطنة الرقمية مرتبطة بالقدرة على تنمية المواطنة العادية بأدوات رقمية و تقنيات تكنولوجية ، ولكن في حقيقة الحال أن الأمر على خلاف هذا.

المواطنة الرقمية مجموعة من الأفكار والمبادئ والبرامج والأساليب التي يحتاج الآباء والمعلمون على استخدام التكنولوجيا ان يعرفوها حتى يستطيعوا توجيه الشباب والطلاب ومستخدمو التكنولوجيا عموماً، حيث تسعى المواطنة الرقمية لإيجاد الطرق المثلى لحماية الأطفال والمراهقين.¹²

يعرف "المواطنون الرقميين" بأنهم أولئك الذين يستخدمون الإنترنت بانتظام وفعالية – أي على أساس يومي، بالإضافة إلى امتلاك المهارات اللازمة لاستخدام التكنولوجيا و إمكانية الوصول إليها.¹³

يمكن تعريف المواطنيين الرقميين حسب كارين موسبرغر" بأنهم أولئك الذين يستخدمون الإنترنت بشكل يومي، لأن الاستخدام المتكرر يتطلب توفر وسيلة وصول منتظمة (غالباً في المنزل)، وبعض المهارات التقنية، والكفاءات التعليمية التي تمكن من تنفيذ مهام مثل البحث عن المعلومات على الويب واستخدامها، والتواصل مع الآخرين عبر الإنترنت... المواطنة الرقمية هي عامل ممكن للمواطنة السياسية".¹⁴

المواطنة الرقمية هي مجموعة من قواعد السلوك التي تُنظم استخدام التكنولوجيا المتنوعة، وتشمل استخدامها في تبادل المعلومات إلكترونياً، والمشاركة الفعالة في الحياة المجتمعية عبر الوسائط الرقمية.

ب. اجرائيا: مجموع السلوكيات والأخلاقيات التي يتحلى بها الفرد أثناء استخدام التكنولوجيات الحديثة: احترام الآخرين، حماية الخصوصية، المشاركة الايجابية في الفضاء الرقمي.

ثانيا: استراتيجيات تعزيز المواطنة الرقمية من منظور الأمن السيبراني:

للمواطنة الرقمية عدة أبعاد تساهم في اعداد مواطن رقمي، يحسن توظيف التكنولوجيات الحديثة والأنترنت بالتحديد، بشكل مسؤول وقانوني، ومن بين هذه الأبعاد الأمن السيبراني. بحيث تعتمد الدول والحكومات عدة استراتيجيات لتحقيق البعد الأمني وتعزيز المواطنة الرقمية في المجتمعات.

1. استراتيجيات قانونية وتشريعية:

تعد الجرائم السيبرانية من أهم المخاطر الجديدة التي تستهدف المستخدمين والخدمات الإلكترونية في الفضاء الأزرق، من سرقة الهوية الرقمية والبيانات الخاصة للمستخدم، اختراق وتخريب البنى التحتية للاتصالات وتكنولوجيا المعلومات... الخ. فكان لابد من تبني استراتيجيات الأمن السيبراني من طرف الحكومات والأفراد، لتعزيز حماية وسرية وخصوصية البيانات الشخصية من الهجمات السيبرانية وغيرها من الأخطار السيبرانية.

المواجهة الفاعلة للجرائم السيبرانية تستلزم اتخاذ جميع التدابير اللازمة لحماية المواطنين من المخاطر المحتملة في مجالات استخدام الانترنت وتطبيقاتها المختلفة. ويتحقق ذلك بالاستخدام الأمثل لتكنولوجيات، مما ينعكس على ممارسة المواطنة في شكلها الرقمي بأسلوب عقلائي وفعال، باعتبارها مجموعة الضوابط والمعايير والمبادئ المتبعة في الاستخدام الأمثل والقويم للتكنولوجيا، مما يساهم في تعزيز الأمن السيبراني للمجتمعات.

باعتبار ان الترسنة القانونية الهيكل المنظم لأمن المجتمعي، يستلزم على الدول والحكومات مواكبة التحولات التي رافقت ظهور مجتمع المعلومات، بوضع برنامج لتطوير الإطار التشريعي الملئم لأمن المعلوماتي السيبراني، وحماية الخصوصية والهوية الرقمية للمواطنين لتأطير آليات تكوين مواطنة رقمية ناجعة تنعكس على وعي المستخدمين داخل الفضاءات الرقمية.

تعد هذه البرامج بمشاركة من الاطراف المعنيين، وهم ذوي الخبرة في القطاع الحكومي والخاص والأكاديمي، ومؤسسات المجتمع المدني، مع الاسترشاد بالخبرات والتجارب والبرامج الدولية ذات الصلة. حيث أن وجود أي فراغ تشريعي بشأن الجرائم السيبرانية قد يضر ضررا بالغاً بمنظومة المعاملات الإلكترونية والخدمات الإلكترونية.¹⁵

عالجت مصالح المديرية العامة لأمن الوطني الجزائري المختصة في مكافحة الجرائم المتصلة

طبيعة القضايا المسجلة	السنة	عدد القضايا المسجلة
الابتزاز والتهديد والتشهير والمساس بالحريات الشخصية والحياة الخاصة	2021	2838 قضية
نشر المعلومات الزائفة، القرصنة والتشهير والتحرش الإلكتروني والنصب والاحتيال	2022	4600 قضية
بتكنولوجيات الإعلام والاتصال قضايا عديدة من الجرائم الإلكترونية:	بداية 2023	500 قضية

جدول(01): الجرائم الإلكترونية المعالجة من طرف مصالح المديرية العامة لأمن الوطني الجزائري المختصة في مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال. (جريدة الشروق اليومي ، 2023، صفحة 08)

وتجسيدا لذلك باشر المشرع الجزائري في اعداد قوانين خاصة لمجابهة الجرائم الالكترونية انطلاقا من نظام العقوبات في القوانين الدولية للجريمة الإلكترونية، باعتبار الجزائر من بين الدول التي دخلت مصاف الإدارة الإلكترونية والعالم السيبراني، وعليه حاولت تأمين الفضاء المعلوماتي لكل الناشطين فيه، وذلك من خلال مراجعة التشريعات والنصوص القانونية المتعلقة بالأمن السيبراني.¹⁶

استدرك المشرع الجزائري في السنوات الأخيرة ولو نسبيا الفراغ القانوني في مجال الجريمة الالكترونية، وذلك لما أصدر القانون 04-15 المتضمن تعديل قانون العقوبات، حيث خصص قسمه السابع مكرر للمساس بأنظمة المعالجة الآلية للمعطيات، وتضمن ثماني مواد، اذ تعلقت المادة 394 مكرر بمعاينة كل من يدخل أو يبقى عن طريق أو جزء من منظومة للمعالجة الآلية

للمعطيات أو يحاول ذلك، أما المادة 394 مكرر¹ فنصت على معاقبة كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها.¹⁷

وصدر قانون: 04-09 المتعلق بالجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها سنة 2009، وأشار الى جرائم المساس بالأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية.

وأما من ناحية الجانب الدولي: هذا بالدول لوضع تشريعات لمواجهة ذلك وكانت بداية انفتاحها على القانون الجنائي والذي يرسخ بداية هذه الفكرة قانون جرائم المعلوماتية الفرنسي الصادر سنة 1988م ويحمل الرقم 19 وما تبعه من قوانين أخرى ذات صلة، ومنها التشريع الفرنسي الصادر في 4 أوت 1994 م، المسمى بقانون Toubon، ومن ثم توالى الدول في سن القوانين والتشريعات.¹⁸

ومن الدول العربية: التي اجتهدت في ذلك قانون الجرائم الإلكترونية الأردني رقم 27 لسنة 2015 ، والقانون الاتحادي لدول الإمارات رقم 2 لعام 2006، بشأن مكافحة جرائم تقنية المعلومات، والنظام السعودي لمكافحة جرائم المعلوماتية الصادر سنة 2007م.¹⁹

ويؤكد البروفيسور علاء عبد الرزاق السالمي في كتابه المدخل الى الذكاء الاصطناعي السيبراني ان المشرعين بصورة عامة لم يستجيبوا بعد للتطور التقني، وقد تكون النصوص الجنائية التقليدية قابلة للتطبيق على جرائم الحواسيب، وفي حالة كونها مناسبة فلا بد عندئذ من ملء الفراغ التشريعي في هذا المجال، حيث لا بد أن يكون للجريمة في نطاق المعلوماتية ساعيا نحو وظيفتي العقوبة من ردع عام الى ردع خاص، وبكل وضوح، وصولا الى تقليص القاعدة الاجتهادية.²⁰

2 استراتيجيات تربوية وأخلاقية :

من أجل رفع مستوى الوعي بالأمن السيبراني وتجنب المخاطر السيبرانية وتقليل آثارها، اعتمدت الدول والحكومات استراتيجيات تربوية وأخلاقية لبناء جيل واع تكنولوجيا ومكتسبا لثقافة رقمية تساعد في اكتساب اللياقة والسلوك الرقمي الرشيد مع التكنولوجيات الحديثة.

بحيث أكدت نتائج دراسة الباحثة علياء عمر كامل فرج المعنونة ب: "دواعي تعزيز ثقافة الأمن السيبراني في ظل التحول الرقمي": الزامية تثقيف الطلبة بالممارسات التي تحقق الأمن السيبراني من خلال تضمينها في المقررات والمناهج الدراسية في كافة المراحل التعليمية، تعميم النهج والاستراتيجيات التي تتيح لطلبة تعزيز أمنهم وأمن مجتمعاتهم.²¹

تعد عملية دمج التربية الرقمية أو ما يسمى بالمواطنة الرقمية كوسيلة تربوية معاصرة لتثقيف الأجيال المستقبلية بالأمن السيبراني، وتكوين مواطن رقمي واعي بحقوقه وواجباته، بحيث يؤكد العديد من الباحثين أن المواطنة الرقمية له علاقة قوية بالمنظومة التربوية والتعليمية، وأصبحت آلية استراتيجية للنظم التربوية. بحيث تعرف المواطنة الرقمية أنها: "إعداد التلاميذ والطلاب لاستخدام تكنولوجيا الحاسوب بطريقة فعالة ومناسبة، من خلال تنمية معارفه ببرامج معالجة النصوص، وبرمجيات الاتصال المختلفة وتغرس فيهم مفهوم المواطنة الرقمية الصحيحة وكيفية استخدامها بطرق مناسبة.²²

تؤكد دراسة احدى الدراسات أن المعلمين الذين يعتمدون على دمج التكنولوجيا في عاداتهم اليومية أو المهنية كانوا أكثر فعالية في تعزيز قضايا المواطنة الرقمية والسلامة على الإنترنت داخل الصف، مثل المناقشات مع الطلاب أو تعليم الأطفال السلوكيات الأخلاقية عند التنقل على شبكة الإنترنت.²³

ففي دول متقدمة عديدة مثل بريطانيا والولايات المتحدة وكندا يدرس الطلاب في المدارس مواضيع خاصة بالمواطنة الرقمية في إطار منهج التربية الرقمية. فالمواطنة الرقمية مشروع رسالته إعداد

مجتمع مؤهل للتعامل مع القضايا الإلكترونية بنشر ثقافة الأمن الإلكتروني بين مختلف المراحل العمرية في المجتمع. وللمواطنة الرقمية في السياق التربوي اهداف محددة، أهمها:²⁴

✓ توظيف التقنية في الطرق الصحيحة: ووفقا لقواعد أخلاقية سليمة، مع مراعاة الضوابط الدينية والقانونية، والتي ستعمل على الحد من سلبيات التقنية على المجتمع.

✓ تحسين مخرجات التعلم: بحيث تكون التكنولوجيا المطبقة مفيدة لعملية التعلم وتحسن مخرجاتها لدى الطالب واعداده ليتفاعل مع المستجدات الرقمية بطريقة سليمة ومفيدة بحيث لا يقع تحت طائلة القانون.

✓ تنمية الأداء الأكاديمي للطالب بما يتناسب مع مجريات العصر الرقمي المحيط به والتحول للتعلم الإلكتروني.

✓ تعرف الطالب الحقوق والمسؤوليات الرقمية في بيئة المدرسة وسلوكياته مع زملائه وتعامله مع الأجهزة والنفاذ الى خدمات الأنترنت، وكذلك خارج البيئة المدرسية.

✓ تدريب الطالب على أن يكون مواطن رقمي يتواصل مع مجتمعه المحيط به محليا وعلى مستوى العالم بنفس الكفاءة والاتقان.

✓ نشر ثقافة التعامل الحضاري مع التكنولوجيا الحديثة والأبعاد القانونية لاستخدامات العالم الافتراضي، وتعرف قواعد الأمن السيبراني.

✓ الربط بين الهوية الرقمية وهوية الدول وقيمها الأصلية وهو هدف توعوي لكي لا يقع الطالب تحت سيطرة رقمية معينة، حيث أن استخدام الأنترنت يترك أثارا تبقى مع الشخص فترات طويلة وقد تؤثر على انتمائه الوطني.

✓ الرقابة الذاتية عن طريق تحويل مفهوم الرقابة المشددة وانعدام الخصوصية الى مفهوم الرقابة الذاتية وفق ضوابط الشريعة الإسلامية والقيم الاجتماعي .

قد قامت المفوضية الأوروبية the European Commission بتطوير برنامج أطلق عليه برنامج الإنترنت الأكثر أماناً The Safer Internet Programme يهدف إلى تمكين الشباب عبر الإنترنت وحمايتهم، من خلال تعزيز الاستخدام الآمن والمسؤول للإنترنت وغيرها من تقنيات الاتصال، وأيضاً من خلال محاربة المحتوى والسلوك الغير القانوني والضار عبر الإنترنت.

تم تضمين موضوعات المرتبطة بـ "السلامة على الإنترنت" في مناهج المدارس الوطنية في معظم دول الاتحاد الأوروبي، فخلال العامين الدراسيين 2007/2006م و 2008/2007م أدرجت هذه الموضوعات في المناهج الدراسية الموجودة في أكثر من 80% من البلدان الأوروبية. يشمل تعليم "السلامة على الإنترنت" في المدارس الأوروبية مجموعة متنوعة من الموضوعات أهمها: السلوك الآمن عبر الإنترنت، قضايا الخصوصية عبر الإنترنت، قضايا التحميل من الإنترنت وحقوق التأليف والنشر، التعدي عبر الإنترنت الاستخدام الآمن للهواتف النقالة والتواصل مع الغرباء.... الخ.

في الدول العربية: وبالتحديد في مصر تبنت وزارة التربية سياسة نشر ثقافة الأمان الإلكتروني في المدارس، حيث تركز وزارة التربية والتعليم على تضمين موضوعات السلامة على الإنترنت في مناهج التعليم بالمراحل الابتدائية والإعدادية والثانوية.

في السعودية: أطلقت وزارة التعليم "برنامج فطن" سنة 2015م، وهو برنامج وطني وقائي يهدف الى اكساب الطلاب في المرحلة المتوسطة والثانوية مهارات التعامل الذكي والعقلاني مع التكنولوجيات وما تحويه وسائل الاتصال الرقمي من توجهات ومعتقدات فكرية.

ثالثاً : المجتمع الدولي وتحديات تحقيق الأمن السيبراني :نحو ارساء مواطنة رقمية فعالة :

انصب اهتمام الباحثين على موضوع المواطنة الرقمية وما يرافقها من مفهوم ملازم يتعلق بالأمن المعلوماتي، بعد أن أصبحت هذين المفهومين حقيقة واقعة في ظل ولادة مجتمع المعلومات و إمتداد نسيجه الشبكاتي على مساحة واسعة من النشاط الانساني.

كانت اقتراحات الباحثين شتى وعديدة، حاول من خلالها تشكيل الاطار العام لمفهوم المواطنة في ظل التأثيرات و التحديات السريعة و المتلاحقة لحضور الخطاطة المعلوماتية على هيكلية المجتمع وزخم التحولات التي باتت بصماتها واضحة على ممارسات أفراد.

لقد حدثت النقلة الجديدة للإنسان المعاصر فلم يعد ذلك المواطن المقيم على رقعة جغرافية معينة ويتقاسم ثقافة و عادات و تقاليد توارثها عن الآباء و الاجداد ، كانت هذه النقلة باتجاه أنطولوجيا رقمية ، افتراضية لا تنصاع بسهولة الى سرديات الزمان و المكان حيث اندمجت أدوات الاتصال مع التقنيات المحوسبة لتنتج مناخا من نمط جديد، امتزجت فيه الحوسبة مع بيئة تواصلية ثرية بالمؤثرات المرئية و الصوتية، فاصطنعت مجتمعات وجماعات رقمية بدأت تتواصل و تتقاسم ثقافات و عادات و العديد من الاحتياجات تلك الجماعات التي جعلت من الفضاء الرقمي موطنًا تقيم فيه، متحولة من فضاءها الاجتماعي التقليدي²⁵

من هذا المنطلق بات لزاما على المجتمع الدولي المتمثل في كافة مجتمعاته وهيئاته و كياناته الرسمية للبحث عن حماية بيانات هذه الكيانات و خصوصيات هؤلاء الأفراد و الجماعات ، كتحدٍ لاستتباب أمن سيبراني حقيقي من أجل حماية المواطن المتواصل، الحاضر في قلب الثقافة الرقمية ووسائطها الحديثة ففي هذا الصدد عمل المجتمع الدولي على اصدار عدة اجراءات تنظيمية وتشريعية لتعزيز الأمن السيبراني وحماية المواطنة الرقمية من الانتهاك ، وكذلك تعزيز الاستخدام الآمن و الفعال لأدوات المعلومات و الاتصالات، من بين هذه الاجراءات و القرارات نذكر :

أ- إتفاقية المجلس الأوروبي بشأن جرائم الأنترنت :

اعتمد المجلس الأوروبي الطابع الدولي لجرائم الكمبيوتر منذ 1976 ، وفي العام 1996 أنشأت اللجنة الأوروبية لمشاكل الجريمة (CDPC) لجنة خبرات للتعامل مع مشكلة الجريمة السيبرانية ، عملت اللجنة بين العامين 1997 و 2000 على مشروع الاتفاقية التي اعتمدها البرلمان الأوروبي في الجزء الثاني و تهدف الاتفاقية الى :

- تعيين نظام سريع و فعال للتعاون الدولي فيما يخص الجرائم السيبرانية

- الحفاظ بشكل سريع على البيانات المخزنة على أجهزة الكمبيوتر و حفظها و الافضاح الجزئي عن حركة هذه البيانات المخزنة على أجهزة الكمبيوتر
- جمع معلومات عن حركة البيانات و عن إمكانية وجود تدخل في محتواها
- تتضمن أيضا الاتفاقية المبادئ العامة المتعلقة بالتعاون الدولي في المواضيع التالية :تسليم المجرمين ، المساعدة الدولية المتبادلة في جمع حركة المعلومات و اعتراضها
- الاجراءات المتعلقة بطلبات المساعدة المتبادلة في غياب الاتفاقيات الدولية.²⁶

ب/ مجموعة الدول الثماني (G8)

عملت مجموعة الدول الثمانية (G8) على إيجاد حلول دولية موحدة وفعالة، كتنظيم مؤتمر "مبادئ وخطة العمل بشأن الجريمة ذات التكنولوجيا العالية و جرائم الكمبيوتر سنة 1997، وكذلك مؤتمر " توافر مبادئ البيانات الأساسية لحماية السلامة العامة" إضافة الى بيان المجموعة الذي تكلم عن نظم حماية المعلومات سنة 2002.

ومن جملة التوصيات التي إتفقت عليها دول الثماني الكبرى (G8) في العديد من المعاهدات التي إبرمتها من أجل تحقيق الأمن السيبراني ومواطنة رقمية فعالة نلخصها فيما يلي :

- يتعين على الدول أن تجرم الانتهاكات على حقوق الغير ، على الشبكة العنكبوتية التي تستوجب العقوبات الجزائية و أن تعالج المشاكل المتعلقة بالتحقيقات القضائية بالتدريج الفعال لمنع الجريمة ، و اقامة تعاون دولي في ما يتعلق بمكافحة هذه الانتهاكات الحاصلة على البيئة الرقمية.
- ينبغي للدول ان تتخذ خطوات رادعة لمنع الجريمة ذات التقنية العالية ويشمل ذلك :
- التعاون مع القطاع الصناعي لضمان أمن الشبكات و نظم الاتصالات ، وإيجاد الآليات المناسبة عند تعرض المواقع الالكترونية للهجمات.

- سن قوانين و تدابير أخرى و تنفيذها لضمان حماية ملائمة لحقوق الملكية الفكرية ضد التزوير و القرصنة.
 - تحديد المشاكل المحتملة و معالجتها في المستقبل التي قد تنتج عن التطورات في مجال تكنولوجيا المعلومات.
 - نشر الوعي المعلوماتي فيما يخص مواضيع الجريمة ذات التقنيات العالية.
 - يتوجب على الدول العمل المستمر على اقتناء التكنولوجيات الملائمة و التطوير المستمر للخبرات و القدرات في مجال التحقيق و الادعاء العام من أجل ملاحقة المجرمين الذين يستخدمون تكنولوجيات الاتصال لارتكاب جرائمهم.
 - على الدول تشجيع وضع القوانين و تنفيذ تدابير لتوفير حماية فعالة للأطفال من جميع أشكال الاستغلال الجنسي على المنصات الرقمية وشبكة النت عموماً.
- وفي نفس الصدد إنعقدت العديد من المؤتمرات الأوروبية و اللقاءات الدولية نذكر منها :
- المؤتمر العالمي الرابع " الفضاء الالكتروني " الذي انعقد في مدينة لاهاي بهولندا خلال الفترة 16-17 أبريل 2015
 - مبادرة عمل وارسو: انعقد سنة 2019 في سول وحضره ممثلو أكثر من 40 دولة ، جاء تحت شعار أمن الفضاء السيبراني تحمور النقاش فيه حول استراتيجيات الردع و صد الهجمات الالكترونية.²⁷

ج/ مؤتمرات و لقاءات عربية :

- مؤتمر قمة الأمن السيبراني -مملكة البحرين 22-23 أكتوبر 2014 ناقشت هذه القمة الموضوعات التالية :بحث سبل اعادة الأمن و استراتيجيات تكنولوجيا المعلومات ، واعادة تعريف

المخاطر و تنفيذ أفضل الممارسات لتخفيف مخاطر مواقع التواصل الاجتماعي و استراتيجية مواجهة التهديدات المتنقلة و استغلال الأطفال.

● المؤتمر الدولي لمكافحة الجرائم المعلوماتية الذي نظمتها جامعة الامام محمد بن سعود في المملكة السعودية في الفترة 10- 12 نوفمبر 2015

● قمة الأمن السيبراني " في الدوحة بالشراكة بين مؤتمر ميونخ للأمن و اللجنة الوطنية القطرية للأمن السيبراني 2020 بمشاركة ممثلين رفيعي المستوى عن حكومات ومؤسسات دولية و أعمال تجارية و اوساط أكاديمية و عسكرية ل مناقشة قضايا الأمن الاقليمي و العالمي و زيادة الوعي السيبراني.

غير أن جهود المجتمع الدولي لتعزيز وتكريس الامن السيبراني لبلوغ مواطنة رقمية فعالة ،تعتبرها بعض العوائق و التحديات ، مما يضطر به الى مضاعفة الجهود وتعزيز التعاون الفعال بين الدول و الحكومات للحيلولة من الوقوع في شرك الهشاشة المعلوماتية وذلك بالتحصين من الاختراق المعلوماتي و الحماية من الجرائم السيبرانية ، التزاما بحماية بيانات هيئاتها و مؤسساتها الرسمية و خصوصيات أفرادها، ومواطنيها الرقميين ، ومن بين هذه العوائق و التحديات نذكر :

● التطور التكنولوجي في مجال الانترنت و الاتصالات : وهو ما يفرض على الأجهزة الامنية المختصة بمسيرة هذا التطور ، سواء من حيث اكتساب التكنولوجيا و التقنية أو من حيث التمكن من استخدامها و استثمارها بالشكل اللازم ، وهذا ما يرهق ميزانية هذه الدول فبذلك يجب توفير كل الامكانيات المادية و البشرية اللازمة لتحقيق الأمن السيبراني.

● من بين الاشكالات التي تساهم في انتشار الجريمة الالكترونية هو الافلات من العقاب و التأخر في تفعيل القوانين مما يعطي للمجرم فرصا لتكرار جرائمه كما أنه من الواجب أن تتكيف النصوص القانونية مع التغيرات الحاصلة في هذا المجال ،مما يستلزم انشاء محاكم متخصصة بالجرائم الالكترونية.

● الاستخدام الواسع لشبكات التواصل الاجتماعي وما أنجر عنه من ارتفاع كبير في الجريمة الالكترونية وانتهاك الخصوصية و نخص بالذكر تلك الجرائم المتعلقة ب :الغذف ، التحرش الجنسي، استغلال القصر ،اختراق الحسابات الشخصية و غيرها من الجرائم مما يتطلب وضع استراتيجيات جد محكمة لضمان الأمن المعلوماتي عند استخدام هذه المنصات الاجتماعية.²⁸

أصبحت القدرات التواصلية والاجتماعية مهمة جداً في المجتمع الرقمي المتطور. فبالإضافة إلى القدرة على استخدام التقنيات الرقمية والتفاعل معها بفاعلية، يجب على المواطن الرقمي أيضاً أن يمتلك مهارات التواصل والتعامل مع الآخرين عبر الإنترنت، بما في ذلك فهم ثقافات الإنترنت والتعامل مع الصراعات والتوترات التي تنشأ عبر الشبكة العنكبوتية.

فالتحدي القائم على المواطن الرقمي أن يتعلم كيفية التواصل بشكل فعال عبر وسائل التواصل الاجتماعي والبريد الإلكتروني، وأن يفهم أساليب الاتصال والتفاعل الرقمي المناسبة في المواقف المختلفة، بما في ذلك الإدارة الذاتية والتعامل مع الآخرين وتقديم الردود السليمة والمناسبة.

وعلاوة على ذلك، يجب على المواطن الرقمي أيضاً أن يكون قادراً على تحليل البيانات والمعلومات التي يجمعها عبر الإنترنت وفهم كيفية استخدامها بطريقة صحيحة ومسؤولة. ويمكن لهذه المهارات أن تساعد المواطن الرقمي على اتخاذ القرارات الصحيحة والمسؤولة والتفاعل بشكل فعال مع المجتمع الرقمي.

الخاتمة :

إن عملية تحقيق المواطنة الرقمية بشكل كامل وفعال تتطلب الكثير من الوقت والجهد خاصة مع تزايد استخدام التقنية والانترنت مما يعني زيادة احتمالية التعرض للاختراق والهجمات السيبرانية، ولذلك يتعين على الحكومات والأفراد اتخاذ الإجراءات اللازمة لضمان الأمان والحفاظ على الخصوصية.

يتطلب تحقيق المواطنة الرقمية الكثير من العمل على عدة مستويات، بما في ذلك توفير البنية التحتية الرقمية والتدريب والتعليم اللازم للأفراد والتشريعات والقوانين التي تحمي الحقوق الرقمية

للمواطنين. كما يجب توفير خدمات حكومية إلكترونية آمنة وموثوقة وسهلة الوصول إليها لتمكين المواطنين من الحصول على خدماتهم الحكومية بسهولة ويسر.

ومع ذلك، فإن تحقيق المواطنة الرقمية لا يمكن أن يتم بمعزل عن الأمن السيبراني وحماية البيانات الشخصية، ولذلك يجب أن تتم جميع الخطوات والإجراءات بطريقة تضمن حماية الأفراد والحكومات من التهديدات السيبرانية. مما يلتزم العمل على تحسين الأمان والتشفير والتحكم في الوصول إلى البيانات وتوفير برامج الحماية المناسبة للأفراد والمؤسسات.

بشكل عام، يمكن القول إن تحقيق المواطنة الرقمية يتطلب جهودًا كبيرة وتعاونًا شاملاً بين الحكومات والمؤسسات والأفراد، ولكنها جهود تستحق العناء من أجل توفير بيئة رقمية آمنة وموثوقة للجميع.

التوصيات :

1- تحقيق تعليم يركز على التطبيق العملي: من خلال الانتقال من النظريات الخالصة إلى التطبيق العملي، يمكن للطلاب فهم كيفية استخدام التقنية بشكل آمن ومسؤول، وتنمية مهاراتهم الرقمية.

2- زيادة الانتاج العلمي: من خلال تشجيع الأبحاث والدراسات والكتب والقصص والحوارات التي تعزز المواطنة الرقمية والأمن السيبراني، يمكن للمجتمع الاستفادة من المعرفة والخبرات المتنوعة.

3- تدريب المدرسين المتخصصين: من خلال تأهيل المدرسين بشكل مستمر وتعزيز مفاهيم المواطنة الرقمية والأمن السيبراني، يمكن للمدرسين تزويد الطلاب بالمعرفة اللازمة وتوجيههم لاستخدام التقنية بشكل آمن ومسؤول.

- 4- تنظيم المؤتمرات والفعاليات: يمكن للمؤتمرات والفعاليات في مجال الأمن السيبراني والمواطنة الرقمية أن تساعد على تعزيز الوعي والتعلم، وتشجيع النقاش والتفاعل وتبادل الخبرات والأفكار بين المهتمين والمختصين في هذه القضايا.
- 5- تقييم الموردین: يجب تقييم الموردین وتحديد مدى توافرهم لسياسات الأمن القوية والممارسات الأمنية لضمان أن تكون المنتجات المستخدمة آمنة وموثوقة.
- 6- الدعم الأمني: يجب تقديم دعم أمني كافٍ للمستخدمين من خلال توفير التحديثات الأمنية والإصلاحات اللازمة بشكل فوري في حالة اكتشاف ثغرات أمنية.
- 7- التدريب الأمني: يجب توفير التدريب اللازم للموظفين والمستخدمين لتعزيز الوعي الأمني وتحسين السلوكيات.

المصادر والمراجع:

الكتب:

1. أوس نجيب غالب العوادي، الأمن المعلوماتي السيبراني، مركز البيان للدراسات و التخطيط، العراق، 2016.
2. حسن مظفر الرزوي، فضاء التواصل الاجتماعي العربي، مركز دراسات الوحدة العربية ، بيروت، 2013.
3. حمادة رشدي العاطي، المواطنة الرقمية في السياق التربوي، دار الجنان للنشر و التوزيع، عمان، الاردن، 2011.
4. عبد الهادي فتحي مُجد، مجتمع المعلومات بين النظرية و التطبيق، الدار المصرية اللبنانية، القاهرة، 2007.

5. علاء عبد الرزاق السالمي، المدخل الى الذكاء الاصطناعي السيبراني، المنظمة العربية للتنمية البشرية مصر، 2022

6. فارس مُجّد العمارات، الأمن السيبراني المفهوم وتحديات، دار الخليج للنشر والتوزيع، الأردن، 2022.

7. مُجّد كمال، الإرهاب السيبراني، دار كلیم للطباعة والنشر والتوزيع، مصر، 2022.

8. مُجّد محمود العمري، مدخل الى الأمن السيبراني، دار زهران للنشر، عمان، 2020

المجلات:

1. خليفة وريدة، "اشكالية المواطنة في ظل القيم التكنولوجية الحديثة بين حرية المواطن و الامن السيبراني"، حويلات جامعة الجزائر 01، 2021

2. رندة مدحلي مُجّد بنت مهدي، "مدى تضمين قيم المواطنة الرقمية في مقررات الدراسات الاجتماعية"، مجلة الجامعة الاسلامية للعلوم التربوية و الاجتماعية، 2021

3. الزبير رحايلي مُجّد بلهوشات، "مجتمع المعلومات العربي و الفجوة الرقمية"، مجلة العلوم الانسانية و الاجتماعية، 07(03)، 2012.

4. زيدات يوسف، "مدى استيعاب النصوص التقليدية للسرقة الالكترونية"، مجلة مؤثر حكم القانون ومكافحة الفساد 2019

5. سميرة بارة، " الأمن السيبراني في الجزائر"، المجلة الجزائرية للأمن الانساني، 02(02)، 2017

6. العزيز خلفان احمد عبد العاطي، "تعليم المواطنة الرقمية في المدارس المصرية و الاوروبية"، المجلة التربوية (12)، 2016.

7. على سعدي عبد الزهرة جبير، "المواطنة الرقمية: دراسة نظرية"، مجلة القانون والعلوم السياسية، 7(1)، 2021

8. علي مُجَّد الدهشان، " المواطنة الرقمية : مدخلات للتربية العربية في العصر الرقمي"، مجلة نقد وتنوير(05)، 2016

9. علياء كامل عمر فرج " تعزيز ثقافة الأمن السيبراني في ظل التحول الرقمي"، المجلة التربوية. 2022

10. لامية طالة، "من مجتمع المعلومات الى مجتمع المعرفة :نحو مقارنة مفاهيمية."، مجلة العلوم الانسانية، 2021

11. مونية زوقاي، صبيحة بوخدوني: " التربية على المواطنة الرقمية و تطبيقاتها على المناهج المدرسية"، مجلة السراج في التربية و قضايا المجتمع، 02(04)، 2018.

12. الرسائل والمذكرات:

13. باية سيفون، تأثير تكنولوجيا الاتصال على النشر الالكتروني للصحف اليومية الجزائرية المكتوبة. جامعة الجزائر 03، الجزائر. 2015

14. الحسين شربالي، دور وسائط الاتصال الجديدة في تشكيل المعارف، كلية العلوم الانسانية و العلوم الاسلامية و الحضارة ، جامعة الأغواط، 2021.

مواقع الكترونية:

1. مريم مُجَّد سيد حسن على علام، "القوة السيبرانية في السياسة الخارجية الإسرائيلية تجاه إيران 2010-2020، المركز الديمقراطي العربي، 2023،
https://democraticac.de/?p=93046#_ftn58

2. جورج لبكي: المعاهدات الدولية للإنترنت: حقائق وتحديات، مجلة الدفاع الوطني، العدد 83، لبنان، 2023، <https://www.lebarmy.gov.lb/ar/content>

مراجع أجنبية:

1. Birgit Jæger, Digital Citizenship –A Review of the Academic Literature , Der moderne Staat. Zeitschrift für Public Policy, Recht und Management, 2021, 14(1).

2. Karen Mossberger, Caroline J. Tolbert, Digital Citizenship The Internet, Society, and Participation, Massachusetts Institute of Technology, London, 2008.

3. Martti L eho, P. N. (2015). Cyber Security: Analytics, technology and automation. jyvaskyla, Finland: Springer international Publishing.

الهوامش:

- ¹ محمد كمال، الإرهاب السيبراني، دار كلیم للطباعة والنشر والتوزيع، مصر، 2022، ص 11
- ² مريم محمد سيد حسن على علام، "القوة السيبرانية في السياسة الخارجية الإسرائيلية تجاه إيران 2010-2020، المركز الديمقراطي العربي، 2023، https://democraticac.de/?p=93046#_ftn58
- ³ محمد محمود العمري، مدخل الى الأمن السيبراني، دار زهران للنشر، عمان، 2020، ص 18.
- ⁴ Martti L eho, P. N Cyber Security, Analytics technology and automation, Springer international Publishing, Finland, 2015, p25.
- ⁵ فارس محمد العمارات، الأمن السيبراني المفهوم وتحديات، دار الخليج للنشر والتوزيع، الأردن، 2022، ص 15.
- ⁶ أوس نجيب غالب العوادي، الأمن المعلوماتي السيبراني، مركز البيان للدراسات و التخطيط، 2016، ص 06.
- ⁷ الزبير رحايلي محمد بلهوشات، "مجتمع المعلومات العربي و الفجوة الرقمية"، مجلة العلوم الانسانية و الاجتماعية، 07(03)، 2012، ص 173.
- ⁸ عبد الهادي فتحي محمد ، مجتمع المعلومات بين النظرية و التطبيق، الدار المصرية اللبنانية، مصر، 2007، ص 126.
- ⁹ لامية طالة، "من مجتمع المعلومات الى مجتمع المعرفة: نحو مقارنة مفاهيمية"، مجلة العلوم الانسانية، 2021، ص 176.
- ¹⁰ باية سيفون، تأثير تكنولوجيا الاتصال على النشر الالكتروني للصحف اليومية الجزائرية المكتوبة، أطروحة دكتوراه، جامعة الجزائر 03، الجزائر، 2015، ص 56

¹¹ الحسين شربالي ، دور وسائط الاتصال الجديدة في تشكيل المعارف، كلية العلوم الانسانية و العلوم الاسلامية و الحضارة ، جامعة الأغواط 2021، ص 44 .

¹² على سعدي عبد الزهرة جبير، "المواطنة الرقمية: دراسة نظرية"، مجلة القانون والعلوم السياسية، 7(1)، 2021، ص 5.

¹³ Karen Mossberger, Caroline J. Tolbert, Digital Citizenship The Internet, Society, and Participation, Massachusetts Institute of Technology, London, 2008, p14.

¹⁴ Birgit Jæger, Digital Citizenship– A Review of the Academic Literature , Der moderne Staat. Zeitschrift für Public Policy, Recht und Management, 2021, 14(1), p4

¹⁵ خليدة وريدة، "اشكالية المواطنة في ظل القيم التكنولوجية الحديثة بين حرية المواطن و الامن السيبراني"، حوليات جامعة الجزائر 01، 2021، ص 820

¹⁶ سميرة بارة ، "الأمن السيبراني في الجزائر"، المجلة الجزائرية للامن الانساني، 02(02)، 2017، ص 263.

¹⁷ زيدان يوسف، "مدى استيعاب النصوص التقليدية للسرقة الالكترونية"، مجلة مؤشر حكم القانون ومكافحة الفساد، 2019، ص 2.

¹⁸ علاء عبد الرزاق السالمي، المدخل الى الذكاء الاصطناعي السيبراني، المنظمة العربية للتنمية البشرية ، مصر، 2022 ص 63.

¹⁹ علياء كامل عمر فرج ، "تعزيز ثقافة الأمن السيبراني في ظل التحول الرقمي"، المجلة التربوية، 2022 ص 533.

²⁰ صبيحة بوخدوني، مونية زوقاي ، "التربية على المواطنة الرقمية و تطبيقاتها على المناهج المدرسية"، مجلة السراج في التربية و قضايا المجتمع، 02(04)، ص 120.

²¹ علي مُجّد الدهشان ، "المواطنة الرقمية :مدخلات للتربية العربية في العصر الرقمي". نقد وتنوير(05)، 2016، ص 87.

²² حمادة رشدي العاطي، المواطنة الرقمية في السياق التربوي ، عمان، الاردن : دار الجنان للنشر و التوزيع. 2011، ص 25-26.

²³ رندة مدحلي مُجّد بنت مهدي، "مدى تضمين قيم المواطنة الرقمية في مقررات الدراسات الاجتماعية"، مجلة الجامعة الاسلامية للعلوم التربوية و الاجتماعية، 2021، ص 58.

²⁴ العزيز خلفان احمد عبد العاطي، "تعليم المواطنة الرقمية في المدارس المصرية و الاربوية"، المجلة التربوية (12)، 2016، ص 460-458.

²⁵ حسن مظفر الرزو، فضاء التواصل الاجتماعي العربي، مركز دراسات الوحدة العربية، بيروت، 2013، ص 109.

²⁶ جورج لبكي: "المعاهدات الدولية للإنترنت: حقائق وتحديات"، مجلة الدفاع الوطني، العدد 83، لبنان، 2023،

<https://www.lebarmy.gov.lb/ar/content>

²⁷ جورج لبكي: المرجع السابق.

²⁸ سميرة بارة: مرجع سابق، ص 275.