ISSN: 2253-0347
مجلــة علوم الإنسان والمجتمع
Journal of Human and Society sciences
EISSN: 2602-781X
المجلد: 10 / العدد: 04 / السنة: 2021 / ص ص: 153- 172

الأمن الإنساني والهيمنة الذكية تداعيات الانكشاف المعلوماتي

Human security and intelligent dominance the Consequences of informational exposure

تاريخ الإرسال: 30/ 06/ 2021 تاريخ القبول: 30/ 07/ 2021 تاريخ النشر: 2021/12/30

عبد القادر بودربالة [1]، فضيلة تومي [2]

1 جامعة قاصدي مرباح، ورقلة، الجزائر ، *Email : abdelkaderbouderbala@yahoo.fr*

2 جامعة قاصدي مرباح، ورقلة، الجزائر ، *Email : toumi.fadhila@yahoo.com*

الملخص:

قد يبدو الذكاء الاصطناعي تطويرا تكنولوجيا يساهم في تسهيل حياة الانسان ويساعده على التطور، غير أنه بالمقابل يطرح إشكالات كثيرة على مستوى الأمن الإنساني، خصوصا وأن الهيمنة الذكية هي مستقبل المجتمعات الحديثة كواقع، غير أن البعد الاقتصادي الذي تمثله قيمة البيانات الضخمة وتجارتها الرائجة، والبعد الحقوقي والمؤسسي الذي تمثله جدلية (الحرية/المراقبة) لدواعي مختلفة تحت مسمى الأمني أو حتى الصحي مثل تلك الإجراءات التي اتخذتها بعض الدول في مراقبة المصابين بوباء كورونا مؤخرا، كلها أسباب تدعونا لتأسيس بند الأمن التكنولوجي للإنسان ضمن روافد الامن الانساني لحمايته من الهيمنة الذكية لصالح جهات معينة مهما كان نوعها عبر اخضاعه للرقابة واقتحام خصوصيته أو المتاجرة ببياناته الشخصية.

الكلمات المفتاحية: الهيمنة الذكية؛ الأمن الانساني؛ الانكشاف؛ الذات؛ المعلوماتية.

المؤلف المرسل: عبد القادر بودربالة، *Email : abdelkaderbouderbala@yahoo.fr*

Abstract:

Artificial intelligence appears as a technological evolution that contributes to facilitate human life and solve many problems at the level of human security, especially since intelligent domination appears as the future of modern societies, but the economic dimension represented by the value of Big-Data and its trade, and the legal and institutional dimension represented by the controversial (Freedom / Surveillance) for various reasons, in the name of security or even public health, such as measures taken by many countries as part of the surveillance of people infected by the Corona virus epidemic, all these reasons call on us to establish the technological security clause for humans among the basic notions of human security to protect them of intelligent domination for the benefit of certain parties, whatever the type, by subjecting him to surveillance and invading his privacy or the commercial benefit of his personal data.

Keywords: intelligent dominance; Human security; exposure; self; informatics.

مقدمة:

يرتكز الذكاء الاصطناعي على أسس محاكاة القدرات العقلية والادراكية والحسية للإنسان وقدرته على الاختيار وإجراء حسابات منطقية للتعامل مع البيئة المحيطة اعتمادا على التطور الاستثنائي في تصنيع المعالجات، ويسعى الذكاء الاصطناعي لمحاكاة عدة قدرات أهمها: القدرة على التعلم، استيعاب المعرفة، تحليل اللغة والإدراك وحل المشكلات والابداع والتفاعل الاجتماعي وغيرها من القدرات.

ويتصل التطور السريع لتطبيقات الذكاء الاصطناعي بتعزيز قدرات محركات البحث، وتطوير المساعدات الشخصية القادرة على التعرف على الأوامر الصوتية وتحليلها والاستجابة لها، وتقنيات التعرف عى الوجوه وتطبيقات ترشيح المنتجات التي تستخدمها بعض منصات البيع الالكتروني، بالإضافة للتطور في مجالات الرقابة

والمتابعة والرصد والقيادة الذاتية للسيارات وتصنيع المنازل الذكية، فأصبح بذلك سمة عصر الثورة الصناعية الرابعة بالاندماج المتصاعد بين تطبيقات "ذكاء الآلات" والتفاعلات البشرية لتتغير ملامح المجالات الاقتصادية، الأمنية، الاجتماعية والسياسية بصورة هيكلية.

وتتيح تطبيقات الذكاء الاصطناعي إمكانيات غر مسبوقة في مجالات الرقابة والاستطلاع والتحقق من هوية الأفراد ومكافحة الجرائم ورصد واحتواء تهديدات الأمن الداخلي اعتمادا على تحليل البيانات الضخمة، وهو ما يرتبط بدعم عملية اتخاذ القرار استنادا لفهم أكثر دقة لمعطيات البيئة الداخلية والإقليمية والدولية وتقييم وتوقع توجهات ومواقف المواطنين تجاه القرارات والسياسات التي يتم اتخاذها.

وعلى المستوى الاقتصادي، شهدت عمليات التصنيع والتسويق والمبيعات وخدمة العملاء تحولات جوهرية نتيجة لدمج تقنيات الذكاء الاصطناعي التي تسهم في تعزيز القدرة على فهم الأسواق وتوقع الاتجاهات الاقتصادية وتعزيز الانتاجية والرقابة على الجودة، ومواجهة الاختلالات الكامنة في العملية الإنتاجية، وتعزيز قدرة الشركات على الدعاية والتسويق للمنتجات عبر قراءة أعمق لتفضيلات المستهلكين واحتياجاتهم.

وتثير تقنيات الذكاء الاصطناعي كذلك إشكاليات تتعلق بمدى قبول الأفراد لاتخاذ تطبيقات الذكاء الاصطناعي للقرارات وتقدمهم للخدمات ومدى ارتياحهم للتفاعل مع الآلات بديلا عن البشر، فضلا عن ردود الأفعال الرافضة لاختراق خصوصية الأفراد وتوظيف بياناتهم الشخصية المترتب عن انكشافهم الهوياتي ضمن كم البيانات الضخمة التي يعتمد عليها الذكاء الاصطناعي.

ففي بداية انتشار الانترنت في تسعينيات القرن الماضي ظهرت بعض القوانين والتشريعات التي تحمي بيانات الأفراد المستخدمة عبر الانترنت، وقد اتسمت بيانات الأفراد في تلك الفترة بكونها محدودة وقليلة للغاية، لكن مع التطورات التكنولوجية المستمرة وزيادة اعتياد الأفراد على الانترنت والتقنيات الذكية المختلفة في حياتهم اليومية كالهواتف الذكية وأجهزة انترنت الأشياء والمساعدات الشخصية

والأجهزة التي تعمل بالأوامر الصوتية زاد حجم ونوع البيانات الشخصية التي يمكن الحصول عليها عبر الانترنت.

وامتدت هذه البيانات لتشمل بيانات الأفراد الحيوية خلافا عن الموقع الجغرافي ومكان العمل والإقامة وأي أماكن أخرى يتردد عليها والعديد من المعلومات الشخصية الأخرى، مثل نوعية الأطعمة والمشروبات والملابس والأفلام والكتب والموسيقى التي يفضلها المستخدم وسجل مشترياته كاملا عبر الانترنت، ومواعيد عمله ونومه وغذائه، وتحديد شبكة أصدقائه وأفراد عائلته، وإن أردنا الايجاز فيمكننا القول أن "الأجهزة الذكية تعلم عنا أكثر ما نعلمه عن أنفسنا".

وتكمن الخطورة في أن البيانات هي أساس العامل الرقمي الحالي، وجمعها ضروري للشركات بهدف تحسن الخدمات التي تقدمها لعملائها، سواء خدمات البحث عن التفضيلات أو خدمة الإعلانات أو ترشيحات الأخبار والكتب والأفلام...، فضلا عن كونها البنية الاساسية لتطوير نظم الذكاء الاصطناعي، فهي تحتاج كميات كبيرة من البيانات العملاقة لكي تتعلم القيام بوظائفها، فالبيانات هي أساس عملية التطور التكنولوجي.

إلا أن عملية الحفاظ على هذه البيانات من إساءة الاستخدام هو التحدي الرئيسي الذي يواجه المستخدمين كافة للأجهزة الذكية، سواء الحفاظ عليها من الاختراق والقرصنة وإساءة استخدامها من قبل المجرمين الذي يستطيعون سرقة البيانات الحيوية للأفراد من الأجهزة الذكية وانتحال شخصياتهم الحقيقة في القيام بأعمال إجرامية، أو الحفاظ عليها من إساءة استخدام شركات التكنولوجية لهذه المعلومات لتحقيق مكاسب مالية أو سياسية على حساب خصوصية المستخدمين.

ويتضح الاستغلال المالي لهذه البيانات في تحقيق عوائد مالية من الإعلانات التي تقدمها هذه الشركات، أو في تطوير منتجات ذكية استهلاكية لاستمرار تحقيق الريادة في سوق الأجهزة الذكية، وهو ما يدفع للتساؤل عن حق المستخدم في هذه العوائد والمكاسب المالية العملاقة في إطار حق الأفراد في الاستفادة من بياناتهم الشخصية.

ويتضح الاستغلال السياسي للبيانات فيما كشفت عنه فضيحة شركة Cambridge Analytica ، حيث عمدت هذه الشركة إلى استخدام بيانات الافراد الشخصية على موقع Facebook ودراسة اهتماماتهم وتوجهاتهم في التأثير على العملية الديموقراطية وتغيير توجهات الناخبين، سواء كان ذلك عبر الاستفتاء في بريطانيا على الخروج من الاتحاد الأوروبي أو أثناء الانتخابات الرئاسية الأمريكية سنة 2016.

وعليه، نحاول من خلال هذا المقال تسليط الضوء على تداعيات الانكشاف المعلوماتي، وقد هيكلنا عملنا هذا في عدة نقاط أساسية ومنها تطور تقنيات جمع المعلومات وظهور أنواع جديدة من المعلومات وانتشار تحليل البيانات الضخمة وتقنيات تمييز الهويات الشخصية وظهور الجدل حول ملكية البيانات والوعي بمفاهيم استغلالها، بما يفرض محور الامن الأمن التكنولوجي للأفراد والجماعات في إطار الامن الإنساني الشامل ضد الهيمنة الذكية وتأثيرها على حياة الافراد، كل هذا من خلال البحث عن **تساؤل الحريات والامن الإنساني في عصر الهيمنة الذكية؟ وتداعيات انكشاف الذات المعلوماتي على خصوصية المستخدم وأمنه الرقمي؟**

1. الامن الإنساني، التكنولوجيا والحريات:

برز مفهوم الأمن الإنساني في النصف الثاني من تسعينيات القرن العشرين كنتاج لمجموعة التحولات التي شهدتها فترة ما بعد الحرب الباردة فيما يتعلق بطبيعة مفهوم الأمن، ونطاق دراسات الأمن، إذ أثبتت خبرة الحرب الباردة أن المنظور السائد للأمن وهو المنظور الواقعي لم يعد كافيا للتعامل مع طبيعة القضايا الأمنية ومصادر التهديد فترة ما بعد الحرب الباردة، وبالتالي برزت الحاجة لتوسيع منظور الأمن ليعكس طبيعة مصادر التهديد فترة ما بعد الحرب الباردة. (سلام، 2017)

ويركز مفهوم الأمن على الإنسان الفرد وليس الدولة كوحدة التحليل الأساسية، فأي سياسة أمنية يجب أن يكون الهدف الأساسي منها هو تحقيق أمن الفرد بجانب أمن الدولة، إذ قد تكون الدولة آمنة في وقت يتناقص فيه أمن مواطنيها، بل إنه في بعض الأحيان تكون الدولة مصدرا من مصادر تهديد أمن مواطنيها، إن حماية أمن الفرد

لم يعد مسؤولية الدولة التي ينتمي اليها، وإنما هي مسؤولية العالم بكل أفراده ومؤسساته، نتيجة التطور التكنولوجي الهائل وتعدد مخاطر الجريمة وتجاوزها للحدود الوطنية للدول وظهور مؤسسات وشركات عابرة للحدود. (عدنان، 2016)

لقد أصبح مفهوم الامن الانساني إطارا موسعا للأمن الوطني (أمن الدولة + أمن المجتمع + أمن الانسان) اذ أصبح هذا الاخير يحتوي بالإضافة لحماية الحدود والوحدة الترابية وسيادة الدولة ومصالحها الوطنية والحيوية على ابعاد وظيفية اخرى مرتبطة بحماية حقوق الانسان وحرياتهم وترقيتهم بشكل يمكن ضمان كينونتهم وكرامتهم ومستقبل الاجيال القادمة. (المركز متعدد التخصصات، 2021)

توجد العديد من التهديدات الموجهة للأمن الإنساني التي تركز على أمن الانسان في حياتهم اليومية، والذي يمثل الاهتمام المبدئي والأساسي للبشر، وهذه التهديدات متسعة إلا أنه يمكن ضمها في سبعة فئات رئيسية، أو محاور تمثل أبعاد الأمن، وكل محور يحمل التهديدات الخاصة به وهذه المحاور هي (الأمن الاقتصادي، الأمن الغذائي، الأمن الصحي، الأمن البيئي، الأمن الشخصي، الأمن المجتمعي، والأمن السياسي)، ورغم اتساع قائمة التهديدات لكل محور من المحاور السبعة إلا أننا سنركز على جانب الحريات الذي يعد جانبا من محور الامن السياسي، غير أن ارتباط التهديد بالتكنولوجيات الحديثة للإعلام والاتصال، وما يمكن أن تشكله استخداماتها من تهديدات لخصوصية الافراد والاخطار المحتملة من الافراد والجماعات عبر تلك الوسائط التكنولوجية يدفعنا لتقديم محور آخر وهو الامن التكنولوجي وما يجب أن يتخذ من إجراءات لحماية الافراد سواء من الجانب التقني، التشريعي، حوكمة البيانات، والتعاون المطلوب جنوب-جنوب أو شمال جنوب، خصوصا في ظل التفاوت التكنولوجي بين دول الشمال والجنوب، أو بين من يملك التكنولوجيا وآليات الحماية وبين من يفتقد ذلك.

في هذا الصدد وبعيدا عن المستوى الثاني من الاخطار التي تمثلها التكنولوجيا على حريات الافراد وأمنهم والذي تمثله الجريمة الالكترونية في عمومها (سرقة الهوية، الاختراق، الاستدراج، التنمر، القذف....)، نركز حديثنا حول المستوى الأول لتلك الاخطار وهو اختراق بيانات الافراد وجمعها لأغراض تجارية أو سياسية من قبل الشركات

العملاقة وتهديد حريات الافراد وانتهاك حقوقهم التي تأسست بولوج البشرية العصر الرقمي، خصوصا ما يرتبط ببياناتهم الشخصية، هذه الاخطار تتعاظم بشكل كبير في خضم الهيمنة الذكية لدول ومؤسسات بعينها باستخدام تقنيات الذكاء الاصطناعي. (الحيدري، 2019)

يعرف جون مكارثي (John McCarthy) الملقب بأبي الذكاء الاصطناعي هذا المفهوم على أنه "علم هندسة الآلات الذكية، وبصورة خاصة برامج الكمبيوتر"، حيث إنه يقوم على إنشاء أجهزة وبرامج حاسوبية قادرة على التفكير بالطريقة نفسها التي يعمل بها الدماغ البشري، وتحاكي تصرفات البشر، وبهذا المعنى، فإن الذكاء الاصطناعي هو عملية محاكاة الذكاء البشري عبر أنظمة الكمبيوتر، فهي محاولة لتقليد سلوك البشر ونمط تفكيرهم وطريقة اتخاذ قراراتهم، إذ تتم دراسة سلوك البشر عبر إجراء تجارب على تصرفاتهم ووضعهم في مواقف معينة ومراقبة ردود أفعالهم وأنماط تفكيرهم وتعاملهم مع هذه المواقف، ثم محاولة محاكاة طريقة التفكير البشرية عبر أنظمة كمبيوتر معقدة.(MacCarthy, 1999)

وعلى الرغم من هذا، فإنه لا يمكن أن يطلق هذا المفهوم على أي قطعة إلكترونية تعمل من خلال خوارزمية معينة، وتقوم بمهام محددة، فلكي نطلق هذا المصطلح على نظام إلكتروني لابد أن يكون قادرا على التعلم وجمع البيانات وتحليلها واتخاذ قرارات بناء على عملية التحليل، بصورة تحاكي طريقة تفكير البشر، وهو ما يعني ضرورة توافر ثلاث صفات رئيسية هي: (عبد الله و أحمد حبيب ، 2019)

1. القدرة على التعلم أي اكتساب المعلومات ووضع قواعد استخدام هذه المعلومات.
2. إمكانية جمع وتحليل هذه البيانات والمعلومات وخلق علاقات فيما بينها، ويساعد في ذلك الانتشار المتزايد للبيانات العملاقة (Big Data).
3. اتخاذ القرارات وذلك بناء على عملية تحليل المعلومات، وليس فقط مجرد خوارزمية تحقق هدف معين.

ويمكن تقسيم أنواع الذكاء الاصطناعي إلى أربعة أنواع رئيسية تتراوح من رد الفعل البسيط إلى الإدراك والتفاعل الذاتي، وذلك على النحو التالي: (جاسم، 2019)

1- الذكاء الصناعي الضيق أو الضعيف: وهو أبسط أشكال الذكاء الاصطناعي، حيث تتم برمجة الذكاء الاصطناعي للقيام بوظائف معينة داخل بيئة محددة، ويعتبر تصرفه بمنزلة رد فعل على موقف معين، ولا يمكن له العمل إلا في ظروف البيئة الخاصة به.

2- الذكاء الاصطناعي القوي أو العام: ويتميز بالقدرة على جمع المعلومات وتحليلها، ويستفيد من عملية تراكم الخبرات، والتي تؤهله لأن يتخذ قرارات مستقلة وذاتية، ومن الأمثلة على ذلك السيارات ذاتية القيادة، وروبوتات الدردشة الفورية، وبرامج المساعدة الذاتية الشخصية.

3- الذكاء الاصطناعي الخارق: وهي نماذج تحت التجربة وتسعى لمحاكاة الإنسان، ويمكن هنا التمييز بين نمطين أساسيين، الأول: يحاول فهم الأفكار البشرية، والانفعالات التي تؤثر على سلوك البشر، ويمتلك قدرة محدودة على التفاعل الاجتماعي، أما الثاني فهو نموذج لنظرية العقل، حيث تستطيع هذه النماذج التعبير عن حالتها الداخلية، وأن تتنبأ بمشاعر الآخرين ومواقفهم وقادرة على التفاعل معهم، ويتوقع أن تكون هي الجيل القادم من الآلات فائقة الذكاء.

منذ ظهور مخرجات تكنولوجيا الذكاء الاصطناعي في مختلف المجالات، فإن دور التكنولوجيا أصبح أكثر العوامل المؤثرة في تحديد موازين القوى في النظام الدولي. إذ أن الدول التي تمتلك أدوات التكنولوجيا وتحرص على تطويرها باستمرار تكون فرصها أكبر في ممارسة النفوذ والتأثير في تفاعلات السياسة الدولية، وهذا ما دفع الرئيس الروسي فلاديمير بوتين إلى القول إن "من سيقود الذكاء الاصطناعي سوف يحكم العالم". وهذا يعني أن العالم قد يشهد خلال المرحلة المقبلة تحولا في موازين القوى على الساحة الدولية، خاصة أن هناك قوى إقليمية ودولية عديدة تستثمر بقوة في مجال الذكاء الاصطناعي، في مقدمتها الولايات المتحدة والصين وروسيا والاتحاد الأوروبي، والهند وربما يؤدي التنافس على التفوق في الذكاء الاصطناعي إلى اندلاع صراعات جديدة. (رياض ، 2020)

في هذا الشأن اتت تكنولوجيا شبكة الجيل الخامس من الإنترنت، ليس بوصفها تطورا تقنيا مهما في حد ذاتها، ولكن لأن تأثيرها الاقتصادي المتوقع من الضخامة والقوة، إلى الحد الذي يمكن أن يؤثر في أجزاء منه على توازنات الاقتصاد العالمي، ومنظومة القوة السائدة في شقها التكنولوجي، الاقتصادي والسياسي، ومن المقدر، وفقا لبعض الدراسات أن تصنع التقنية الجديدة ما يزيد على 13 تريليون دولار إضافية من الناتج المحلي الإجمالي العالمي بحلول منتصف العقد المقبل وتوفير 22.3 مليون وظيفة، وإذا كانت أغلب مجالات الحياة ستستفيد منها، فإنه يمكن أن تسهم في نمو الناتج المحلي الإجمالي العالمي للقطاع الصناعي بمفرده بنسبة 4 في المائة أي أقل بقليل من 740 مليار دولار بحلول 2030، وفي استطاعتها على سبيل المثال خفض تكلفة الإنتاج، ومراقبة أدق وأكثر جودة للمنتجات، وتحليل أفضل للعملية الإنتاجية عبر جمع أسرع للبيانات، بما يسمح لخطوط الإنتاج بتفادي إهدار الموارد. (الذكاء الاصطناعي والتمية الاقتصادية، 2019)

على الرغم من هيمنتها التكنولوجية التاريخية، فإن الولايات المتحدة تتخلف حاليا عن الصين وكوريا الجنوبية من حيث جاهزية شبكة الجيل الخامس، فدولة مثل كوريا الجنوبية تخطط لأن يكون 90 في المائة من السكان من مستخدمي شبكة الجيل الخامس بحلول 2026، ومنه تبرز الأهمية التكنولوجية لشبكة الجيل الخامس في إطار الصراع العالمي على احتلال المرتبة الأولى في المنظومة الاقتصادية الدولية.

وعليه تمثل تقنية الاتصال بالجيل الخامس G5 أحد أهم بؤر الصراع بين الصين وأمريكا، حيث من المرتقب أن تكون تلك التقنية بمثابة العمود الفقري للعديد من الصناعات التي أعلنت بكين أنها ستقوم بتطويرها ضمن «صنع في الصين 2025» مثل الذكاء الاصطناعي والحوسبة الكمية، وأتمتة الآلات، والروبوتات، ومعدات الفضاء والطيران، والمعدات البحرية والشحن عالي التقنية، ومعدات النقل الحديثة للسكك الحديدية، والسيارات ذاتية القيادة والمعتمدة على الطاقة الجديدة، ومعدات الطاقة، والمعدات الزراعية، وتطوير الأجهزة العسكرية الجديدة، والمستحضرات الدوائية الحديثة والمنتجات الطبية المتقدمة. (شادي، 2019)

وعليه وضمن هذا الصراع المحتدم للمصالح السياسية والاقتصادية بين قوى اقتصادية من دول وشركات عملاقة حول احتكار التكنولوجيا والتحكم في البنى التحتية لتقنيات متطورة عمودها الذكاء الاصطناعي وشريانها البيانات ثم البيانات، ضمن هذا الإطار يغيب الحديث تماما عن الامن التكنولوجي وعن حماية الحريات والافراد، رغم بعض الأصوات الحقوقية والطبية التي تعارض انتشار هذه التكنولوجيا وتقدم للأخطار التي تمثلها على الانسان.

إن نموذج الصراع المشحون حول تقنية الجيل الخامس بين القوى العالمية خصوصا الولايات المتحدة والصين، يدعونا إلى الغوص في قاع المحيط والتفكير في أسفل جبل الجليد والابتعاد عن جاذبية القمة، إن انبهارنا بالتكنولوجيا ومخرجاتها ينسينا ما نقدمه من ذواتنا، حرياتنا وحقوقنا مقابل هذه الانتهاك الذي نعده امتيازا، وفي حين تتعارك القوى التكنولوجية والاقتصادية العالمية حول التملك والانتفاع تبقى دول ومجتمعات عديدة عل هامش هذا الصراع رغم أنها هي لب الصراع فما التقنية إلا آلة ومن يحركها هو نحن بتفاعلنا وانكشاف ذاتنا الرقمية واندماجنا رغما عنا في منظومة الهيمنة الذكية للتكنولوجيا الحديثة.

تحديات الهيمنة الذكية:

تعمل شركات التكنولوجيا الأميركية الأربع الكبيرة "GAFA": Google، Apple، Facebook، وAmazon من أجل القوة الأميركية وشركات التكنولوجيا الصينية الأربع الكبيرة "BATX": Baidu، Alibaba، Tencent، Shawmi، تسعف المشروع الصيني كي تصبح القوة الأولى في العالم من هنا حتى سنة 2049، لكن الرابط بين GAFA والسلطة السياسية في أميركا أكثر تعقيدا مما هو عليه الحال في الصين، فلقد اعترض موظفو Google على تعاون منظمتهم مع الجيش الأميركي، بينما هذا الأمر غير وارد في النظام الصيني، لكن في الحالتين، يستخدم العملاقان كرأس حربة لتقوية تأثير بلدا المنشأ على العالم.

الذكاء الاصطناعي ليس قضية اقتصادية فقط، ولا هو مجرد الروبوت و Alexa وAmazon الذي يخدمك في منزلك أو يراجع جدول الضرب مع أطفالك، إنه أيضا أداة

سيطرة. فليس صدفة أن أكبر الاستثمارات فيه يقوم بها العملاقان المتنافسان، الولايات المتحدة والصين هي في هذا المجال، ولو أن الصين لها الأولوية فيما يتعلق بالموازنة التي ترصدها لتطويره.

ينبعث الطموح الصيني من استراتيجية الرئيس الصيني Xi Jinping التي تعتمد على استخدام الذكاء الاصطناعي بشكل مزدوج: من أجل ضبط المواطنين داخليا والتحول إلى القوة الأولى في العالم في نفس الوقت، حيث أصبحت الصين قائدة في البحث والتطوير العلمي وتسجل حاليا براءات اختراع أكثر من الولايات المتحدة الأمريكية، ومنه لا تطمئن فاينانشال تايمز ونيويورك تايمز وفورينغ أفيرز للتقدم الصيني في IA المطبق في الميدان المالي والذي يهدد المؤسسات المالية الغربية، وهو ما يبرزه مؤلف Laurant Alexandre- Jean لكاتبيه ؟L' I A va-t-elle aussi tuer la Démocratie François, Copé J.-C. Lattes.

الانكشاف المعلوماتي:

يرتبط المعيار الحقيقي للحكم على شخص، سلوكه أو حتى أداؤه الوظيفي ارتباطا وثيقا بوجود ملف شخصي له على الشبكة الدولية، أيا كان على "موقع فيسبوك، أو تويتر أو موقع لينكد إن". بل يُعدُّ الملف الشخصي، العنصر الذي يلعبُ دورًا محوريًّا في التواصل بين الأفراد داخل نطاق شبكات التواصل الاجتماعي، بل هو على حدّ وصف دانا بويد "بمثابة الشكل السّائد لعرض الهوية الشخصية على شبكات الإنترنت"؛ لما أنه "سيرة ذاتية قصيرة وواضحة تحدّد أهم ملامح شخصية أحد الأفراد" حسب ما ورد لتعريف كلمة "Profil" في قاموس "ويبستر" عام 1968. حتى أنه ساد الاحتكام إلى عدم وجود مثل هذه الملفات إلى اتّهام الشخص بأنه غير سويّ، على المقابل فمن يمتلكون مثل هذه الملفات يتمتعون بقدر كبير من الاستقلاليّة، ومَن يصنع لنفسه ملفًا شخصيًّا مثيرًا للاهتمام فسوف يُنشئ علاقات تواصل أكثر. (أندرياس و ترجمة: سمر، 2020)

وهو ما تحقق فعليا بعد حوادث الاعتداء التي حدثت في الولايات المتحدة الأميركية عام 2012 بعد إطلاق النار العشوائي في إحدى دور السينما في مدينة دنفر فقد كشفت هذه الحادثة عن احتماليّة وضع حدود بصورة أفضل لمجموعة ممن يُحتمل ارتكابهم لجرائم، والحيلولة في وقت مبكر دون وقوع جريمة. فلقد أثبتت الدراسات إلى جانب الانطواء وعزلة هؤلاء الاجتماعيّة كان ثمّة معيار آخر تمثّل في إحجام القتلة بالإجماع عن استخدام وسائل التواصل الاجتماعي. أي غياب الملف الشخصي عنهم وهو ما يشير بطرف خفي إلى حالة من الاندهاش.

وقد حدا هذا الوضع إلى اعتماد مديري شؤون العاملين في الشركات الكبرى، آلية جديدة لاختيار المتقدمين للعمل، بالتأكيد على الملفات الشخصيّة على شبكة الإنترنت، فغياب هذه الملفات عندهم صار يثير الشعور بالاندهاش. وهو ما أكدته دراسة أجراها الطبيب النفسي الكندي ريتشارد بيلونجيه بأن ثمة علاقة وثيقة بين النشاط على شبكة الإنترنت والصحة النفسيّة لدى الشباب، وأن الشباب الذين لا يتواجدون على الإنترنت لساعات عديدة في اليوم، يثيرون الأطباء وعلماء النفس على الشعور بالانزعاج. وهو ما عكس توجُّها معينا في الثقافة الرقميّة، ارتبط بقياس مدى تواجد ملفات للأشخاص على هذه الشبكات، وإشارات إلى وجود أمر يُلفت الانتباه بشكل غريب من الناحية النفسيّة.

لا يستطيع الإنسان اليوم في ظل انتشار الثقافة الرقمية، أن يحافظ (بقدر المستطاع) على خصوصيته أو الاحتفاظ عليها بالكامل، ولو أنه لا يكشف عنها طواعية وأنه ثمة إكراهات غير مباشرة تلعب دور الفاعل فى جعل ذواتنا مكشوفة أو متاحة فى شبكات الإنترنت.

الخصوصية في مواجهة الهيمنة الذكية:

تجمع شركات التقنية العملاقة، مثل غوغل وفيسبوك، قدرًا ضخمًا من المعلومات عن جميع مناحي حياتنا. الغرض الواضح والمعلن أن هذه المعلومات تساعد ببساطة في بيع المنتجات بشكل أفضل، وذلك عن طريق الإعلانات.تشير بعض

الإحصائيات إلى أن هاتين الشركتين بالتحديد قد جمعتا نحو 150 مليار دولار سنة 2017 فقط، جاء أغلبها من الإعلانات التي تستهدف المستخدمين بأشكال مختلفة.

يمكن أن تُستخدَم هذه المعلومات كذلك للتأثير في أوضاعنا الاقتصادية والاجتماعية والسياسية، سواء عن طريق شركات أو حكومات. كلما زاد حجم تلك المعلومات وعمقها، زادت القدرة على التأثير. يستطيع فيسبوك حاليًّا أن يعرف ما اشتريته، وما تفكر في شرائه، وأين كنت، وأين أنت الآن، وأين ستذهب، وهكذا .يمكنه أيضًا أن يعرف لحظات ضعفك ونشاطك وعملك وراحتك، إضافةً إلى قدرته على تحليل توجهاتك السياسية والحزبية ورؤيتك العالم والآخرين من حولك بشكل دقيق. (جوليا و ترجمة: حسان، 2020)

للحصول على تلك المعلومات، يستخدم فيسبوك نشاطك اليومى على الموقع منذ اشتراكك به، وجميع معلوماتك الشخصية، بما في ذلك صورك، وكل محادثاتك، ودائرة معارفك القريبة والبعيدة، وتاريخ تفاعلاتك وتواصلك معهم. فيسبوك يعرف كل ذلك وأكثر عن 2.2 مليار شخص، هو حجم مستخدميه.

يتزامن هذا الكم الهائل من تداول المعلومات مع تطور ملحوظ في مجال الذكاء الاصطناعي و»تعلُّم الآلة«، الأمر الذي يُسهّل عملية جمع المعلومات وتحليلها، بل واتخاذ قرارات وإجراء تعديلات بناءً عليها.

يمكن أن تمنح تلك المعلومات الغزيرة عند دمجها مع تقنية الذكاء الاصطناعي، قدرًا مخيفًا من القدرة على التأثير الاقتصادي والسياسي في يد شركات التواصل الاجتماعي، وقد يجعلها أحيانًا أقوى من الحكومات ذاتها.

المعلومات والبيانات هي العصب الرئيسي للتقنيات الجديدة المعتمدة على الذكاء الاصطناعي وتعلم الآلة، ويمكن لشركات التقنية العملاقة أن تدفع مبالغ طائلة لجمع تلك المعلومات. فعلى سبيل المثال، دفعت فيسبوك 19 مليار دولار لشراء واتساب . والسبب هو أن واتساب أصبح منصة للتفاعل بين ملايين المستخدمين، وهذا التفاعل

يحدد القيمة التسويقية للشركة، ولعشرات الشركات الناشئة الأخرى، وهو ما تسعى خلفه الشركات العملاقة.

لمواجهة هذه التهديدات، جرى تفعيل "قانون حماية المعلومات والخصوصية" الأوروبي(GDPR) ، وهو القانون الذي يعد خطوة حقيقية في عالم حماية الخصوصية، بدايه من يوم 25 ماي 2018، وظهرت المسودة الأولى لهذا القانون في 2012، بدافع الخوف من توغل شركات التكنولوجيا الأمريكية العملاقة، وبخاصة الأربعه الكبار "GAFA": Google، Apple، Facebook، وAmazon ، في الأسواق الأوروبية وحياة الأوروبيين. وبعد مناقشات وصراعات، وافق البرلمان الأوروبي على القانون عام 2016، وقد كان آخر تحديث لقوانين حماية البيانات والمعلومات في 1995، ومع التطور التكنولوجي الكبير، كان لا بد من ظهور تشريعات جديدة تواكب هذا التطور.

جاء القانون في وقت يشهد حاجة حقيقية إلى تشريعات حماية الخصوصية والمعلومات خاصة بعد فضيحة "كامبريدج أناليتيكا"، ويطبق القانون على أي شركة في الاتحاد الأوروبي، أو لو كان لدى الشركة عملاء ومستخدمون في الاتحاد الأوروبي بغض النظر عن مقر الشركة، وبموجب هذ القانون الجديد يحق للأفراد ما يلي:

1. **الحق في الوصول**: يحق للأفراد طلب الوصول إلى بياناتهم الشخصية، والسؤال عن كيفية استخدام بياناتهم من الشركة بعد جمعها، ويجب على الشركة تقديم نسخة من البيانات الشخصية مجانا بصيغة إلكترونية إذا طلب ذلك.
2. **الحق في النسيان**: يحق للأفراد طلب حذف أو وقف استخدام بياناتهم في أي وقت. و قد كانت Google قد تلقت ما يقرب من 650 ألف طلب حذف بيانات شخصية، ومنعها من الظهور على محركات البحث من متضررين من هذا الأمر.
3. **الحق في إمكانية نقل البيانات**: يحق للأفراد نقل بياناتهم من مزود خدمة إلى آخر. ويجب أن يحدث في صيغة مستخدمة بشكل شائع، ويمكن قراءتها.

4. **الحق في المعرفة**: وهذا يشمل جمع البيانات من الشركات، ويجب إبلاغ الأفراد قبل جمع البيانات، يجب على المستهلكين السماح بأن تجمع بياناتهم، ويجب منح الموافقة بحرية ووضوح بدلا من الأسلوب الضمني.

5. **الحق في تصحيح المعلومات وتغييرها**: ويضمن إمكانية تحديث بيانات الأفراد إذا كانت قديمة أو غير كاملة أو غير صحيحة.

6. **الحق في وقف الاستخدام أو منعه**: يمكن للأفراد طلب عدم استخدام بياناتهم للمعالجة، يمكن أن يبقى سجلهم في مكانه، ولكن لا يمكن استخدامه.

7. **الحق في الاعتراض**: يتضمن حق الأفراد في وقف معالجة بياناتهم واستخدامها للتسويق المباشر، لا توجد استثناءات لهذه القاعدة، ويجب أن تتوقف أي معالجة او استخدام بمجرد استلام الطلب. إضافة إلى ذلك يجب توضيح هذا الحق للأفراد في بداية أي طلب اتصال.

8. **الحق في معرفة أي اختراقات**: إذا كان هناك خرق للبيانات يضر بالبيانات الشخصية للفرد، يحق للفرد إبلاغه في غضون 72 ساعة من علمه بالانتهاك.

هناك عقوبات صارمة على الشركات والمؤسسات التي لا تلتزم بالقانون وغرامات تصل إلى 4٪ من الدخل السنوي للشركة، أو 20 مليون يورو، يعني هذا أن شركة مثل Google يصل دخلها السنوي إلى نحو 100 مليار دولار، يمكن أن تضطر إلى دفع غرامة أربعة مليارات دولار، في حالة المخالفة الصارخة للقانون.

يؤثر القانون الجديد غالبا في معظم الشركات، لكن التأثير الأكبر سيكون على الشركات التي تعتمد نماذج أعمالها على جمع بيانات المستهلك واستغلالها على نطاق واسع، مثل شركات التكنولوجيا، وبخاصة مواقع التواصل الاجتماعي، وشركات التسويق والإعلان، ووسطاء البيانات الذين يربطونهم.

بدأ عدد كبير من المستخدمين في الاستفادة من القانون، عن طريق حجب الموافقة على استخدامات معينة للبيانات، أو رفض طلب الوصول إلى معلوماتهم

الشخصية من سماسرة البيانات، أو حذف معلوماتهم من المواقع بالكامل، ويتوقع أن يكون لذلك تأثير كبير في صناعة جمع البيانات واستخدامها وبيعها.

على الجانب الإيجابي، الصلاحيات الجديدة الممنوحة لمفوضي المعلومات في جميع أنحاء الاتحاد الأوروبي تؤدي إلى أن تكون شركات التكنولوجيا وبخاصة معالجي البيانات، أكثر حذرًا بشأن استخدام البيانات القديمة لأغراض جديدة جذريا.

وعلى الرغم من ذلك، ساهم القانون في ترسيخ الفاعلين الكبار المسيطرين، حيث وجدت الشركات الصغيرة الناشئة صعوبة في إقناع المستخدمين بالموافقة على جمع واسع للبيانات، في حين استطاعت شركات مثل Google أو Facebook تنفيذ ذلك وبسهولة مع ملايين المستخدمين.

إنطلاقا من نموذج الاتحاد الأوروبي، يبدو أن هناك دولا تسلحت بالمعرفة الالكترونية وأسست قوات امنية سيبرانية تحميها من حملات الهجوم الالكتروني وتزودها بكل انواع المعلومات، بينما لم تدرك معظم دولنا العربية خطورة الانكشاف المعلوماتي أمام القوى الاقليمية والدولية.

أصبحت المعارك السيبرانية تدور بين الدول المتصارعة والشركات المتنافسة على الشبكة الالكترونية، وباتت صراعات الفضاء السيبراني على المسرح الدولي هي المادة الأكثر قراءة في إعلام اليوم، لكونها تنقل لنا اخبار المعارك الطاحنة بين المتنافسين كما تنقل اخبار فضائح التسريبات و الاختراقات وسرقة البيانات الشخصية.

عندما انتهت الحرب الباردة بدأت القوى الكبرى على الفور تطوير تقنياتها المعلوماتية، وكونت وحدات أمنها الالكترونية، وابتدعت اسلحتها الجديدة لحروب ليست باردة وانما وصفت حينها بحروب القوى الناعمة، وهكذا انتقلت الصراعات المسلحة بين القوى الكبرى في العالم من ميادين القتال الحقيقية الى ميدان القتال الافتراضية على شاشات الحاسبات، قتال تجرى رحاه على شبكات الإنترنت والفضاء الرقمي.

وعلى مقربة منا تطور الدول الاقليمية تقنياتها الالكترونية بشكل متسارع فتقارع بقوات أمنها السيبراني القوى الإقليمية والكبرى. فها هي ايران تحارب الكترونياً على عدة

جهات، وها هي تركيا المستفيدة من عضويتها في حلف شمال الاطلسي، تقتني المعرفة الالكترونية الغربية وتقوم بتطويرها واستخدامها للدفاع والهجوم في مجال الصراعات السيبرانية، اما إسرائيل التي تعد الاولى في المعرفة الالكترونية اقليميا ومن الاوائل عالمياً، فلم تكتف بقيامها بشن هجمات الكترونية على القوى الفلسطينية، اضافة الى ذلك تتجسس اسرائيل على الدول العربية من خلال برنامجها «بيغاسوس» ومن خلال اختراق الامن السيبراني الاسرائيلي لأسرار الدول والمنظمات العربية.

المعرفة الالكترونية ليست ترفا وانما هي ضرورة حيوية للأمم والدول، فالعالم بأسره يدار اليوم بالطرق الرقمية والمعلوماتية، وفي الكواليس تخوض المؤسسات والتنظيمات والدول معاركها الحاسمة، وعليه يتحتم على الدول العربية تعلم وتطوير معارفها الالكترونية لكي لا تبقى تحت وطأة الانكشاف المعلوماتى والهيمنة الذكية للقوى الإقليمية والشركات التكنولوجية، لحماية أمنها وأمن مواطنيها.

خاتمة:

الذكاء الصناعى وإن بدا تطويرا تكنولوجيا يساهم فى تسهيل حياة الانسان ويساعده على التطور، غير أنه يطرح إشكالات كثيرة على مستوى الأمن الإنساني، خصوصا وأن الهيمنة الذكية هي مستقبل المجتمعات الحديثة كواقع، كما أن البعد الاقتصادي الذي تمثله قيمة البيانات الضخمة وتجارتها الرائجة، والبعد الحقوقي والمؤسسي الذي تمثله جدلية (الحرية/ المراقبة) لدواعي مختلفة تحت مسمى الأمني أو حتى الصحي مثل تلك الإجراءات التي اتخذتها بعض الدول في مراقبة المصابين بوباء كورونا مؤخرا، كل هذه الأسباب تدعونا لتأسيس بند الأمن التكنولوجي للإنسان ضمن روافد الامن الانساني لحمايته من الهيمنة الذكية لصالح جهات معينة مهما كان نوعها عبر اخضاعه للرقابة واقتحام خصوصيته أو المتاجرة ببياناته تجاريا، سياسيا، صحيا ... أو غيره.

على صعيد آخر، وفي خضم الصراع الدائر عالميا بين أكبر قوتين تكنولوجيتين حول تجارة البيانات وتطوير برامج الذكاء الصناعي (الصين والولايات المتحدة الأمريكية)،

ولتلافي تبعاتها على المجتمعات تصارع دول متقدمة، شكل الاتحاد الأوروبي عبر سن قوانين لحماية البيانات وخصوصية الافراد من تبعات الهيمنة الذكية وتجارة البيانات الشخصية نموذجا للمقاومة، في حين تبقى العديد من الدول خصوصا منها دول العالم الثالث ومنها الدول العربية بعيدة عن هذا النقاش من أجل التأسيس لحماية مواطنيها تكنولوجيا من هذه الاخطار في بعدها العالمي والمحلي.

كما يمكن أن نشير إلى أن ما يعطيه الافراد من ذواتهم عبر انكشافهم المعلوماتي هو ما يهدد أمنهم التكنولوجي بالدرجة الأولى، ليغذي سيطرة عمالقة الانترنت عبر الهيمنة الذكية للذكاء الصناعي والبرمجيات المتطورة ومن ثم تفعيل رقابتهم واستغلالهم للبيانات الضخمة التي تجمع عن المستخدمين، وبالتوافق من تفعيل الجانب التشريعي والعمل على المبادرات القانونية البينية في شكل اتفاقيات وقوانين ملزمة خصوصا من قبل دول العالم الثالث، يبدو أن التربية على الوسائل الرقمية أو التربية الرقمية هي الخيار الوحيد الذي يجب العمل عليه لتوعية المستخدمين من هذه الاخطار وترشيد استخدامهم للهواتف الذكية والانترنت في العموم.

إن ما مثلته الوسائل التكنولوجية الحديثة والانترنت بما تحتويه من فضاءات، وما أتاحته برامج وتطبيقات الذكاء الاصطناعي من (حرية لامتناهية) ومجالات للتواصل بلا حدود الزمان ولا المكان، تجمع العديد من الأصوات على اعتباره تهديدا للأمن الإنساني في جانبه التكنولوجي، كما أنه أصبح يرمز للاتصال بدل الاتصال، إن تداعيات الهيمنة الذكية في مقابل انكشاف ذوات الأفراد المعلوماتي تدعو المفكرين إلى المطالبة بفضاء رقمي أكثر إنسانية وقيمية وعدالة إذ لا قيمة لتطور يلغي انسانيتنا.

إن انتقالنا للعيش في الفضاء الرقمي لم يكفل لنا الحرية المنشودة والتمتع بحقنا في التعبير وتجسيد ديموقراطية الاتصال بل أفقدنا أهم شروط التفكير والتميز أفقدنا خصوصيتنا ودفعنا لتقديم ذواتنا عبر الوسائط الرقمية المختلفة مدفوعين بتكنولوجيا مبهرة تقودها التطبيقات الذكية، إن ثروة العصر الحالي هي البيانات الضخمة التي تتصارع قوى عالمية مختلفة لتملكها واستغلالها أمنيا واقتصاديا لتعكس مرآة الحقيقة صورة مطابقة للهيمنة السائدة خارج الفضاء الرقمي، هيئات ومنظمات دولية معطلة،

حروب، انتهاكات، صراع، كبت للحريات... ففي اعرق ديموقراطيات العالم تعرف الآلة ومن يسيرها اليوم عن ذوات أفرادها أكثر مما يعرفون هم عن أنفسهم بفضل هيمنة الذكاء الصناعي في مقابل انكشاف ذواتنا المعلوماتي.

قائمة المراجع:

1. **الذكاء الاصطناعي والتمية الاقتصادية**. (2019). مؤسسة الوراق للنشر والتوزيع.
2. أنغوين جوليا ، و البستاني ترجمة: حسان. (2020). **سلطة شبكات التعقب عبر وسائل الاتصال والانترنت**. بيروت، لبنان: الدار العربية للعلوم ناشرون.
3. برنارد أندرياس، و منير ترجمة: سمر. (2020). **عصر نهاية الخصوصية**. القاهرة: دار صفصافة للنشر.
4. حاجي جاسم. (2019). **الذكاء الاصطناعي**، مستقبل البشرية. Diamond للنشر والتوزيع.
5. زينب الحيدري. (2019). **الأمن السيبراني: النخاطر، التحديات، المواجهة.** قطر: دار الشرق للطباعة والنشر والتوزيع .
6. سميرة سلام. (2017). **تحديات الأمن الانساني في عصر العولمة** . الامارات العربية المتحدة: دار الحامد للنشر والتوزيع.
7. عبد الوهاب شادي. (2019). **حروب الجيل الخامس**: أساليب التفجير من الداخل على الساحة الدولية. الامارات العربية المتحدة: مركز المستقبل للأبحاث والدراسات المتقدمة.
8. قهوجي رياض . (2020). **القوات الجوية وحروب المستقبل**: مفاعيل تقدم التكنولوجيا والذكاء الاصطناعي. الدار العربية للعلوم ناشرون.

9. للبحث في حسن الأداء والتنافسية المركز متعدد التخصصات. (2021). **وقائع المؤتمر الدولي الافتراضي: الأمن الانساني في ظل التحديات العالمية المعاصرة**. المغرب: جامعة محمد الخامس.

10. موسى عبد الله، و بلال أحمد حبيب . (2019). **الذكاء الاصطناعي، ثورة في تقنيات العصر. المملكة العربية السعودية:** المجموعة العربية للتدريب والنشر.

11. ياسين مصطفى عدنان. (2016). **الأمن الانصاني والتنمية:** مؤشرات الهشاشة وفاعلية السياسات. العراق: دار أمجد للنشر والتوزيع.

12. John MacCarthy .(1999) .**Electronic Transactions on Artificial Intelligence** .Useful counterfactuals.