المسابقة البحثية للكوادر الشرطية العربية
في مجال حقوق الإنسان في العمل الأمني

حقوق الإنسان الرقمية
والشرطة الرقمية

إعداد

أغسطس ٢٠٢١م

قَالَ تَعَالَى:

﴿ وَإِذْ قَالَ إِبْرَاهِيمُ رَبِّ اجْعَلْ هَـٰذَا بَلَدًا آمِنًا وَارْزُقْ أَهْلَهُ مِنَ الثَّمَرَاتِ مَنْ آمَنَ مِنْهُم بِاللَّـهِ وَالْيَوْمِ الْآخِرِ ۖ قَالَ وَمَن كَفَرَ فَأُمَتِّعُهُ قَلِيلًا ثُمَّ أَضْطَرُّهُ إِلَىٰ عَذَابِ النَّارِ ۖ وَبِئْسَ الْمَصِيرُ﴾

صدَقَ الله العَظِيم

سورة البقرة: الآية ١٢٦

شكر وتقدير:

الشكر والتقدير للمركز العربي الإقليمي للأمن السيبراني (ARCC) التابع للاتحاد الدولي للاتصالات (ITU)، والشبكة العربية للمؤسسات الوطنية لحقوق الإنسان، والمكاتب المركزية الوطنية للشرطة العربية (الإنتربول)، على التعاون مع الباحث بتوفير بعض الوثائق، ودعم استبيان " قياس وعي وجاهزية الكوادر الشرطية العربية للتعامل مع قضايا حقوق الإنسان الرقمية "، المرفق بالدراسة.

والشكر والتقدير موصول لمجلس وزراء الداخلية العرب، ووزارة الداخلية بجمهورية مصر العربية على مبادرتهما الكريمة والطموحة بتنظيم هذه المسابقة البحثية للكوادر الشرطية العربية في مجال حيوي جداً، وهو "حقوق الإنسان في العمل الأمني".

الإهداء:

إلى كافة منتسبي الأجهزة الشرطية والأمنية العربية، وأصحاب القرار، والجهات المعنية بوضع الاستراتيجيات والسياسات والخطط التنفيذية لحماية وتعزيز حقوق الإنسان في الدول العربية.

حقوق الإنسان الرقمية والشرطة الرقمية

ملخص:

شهدت المجتمعات العربية ـ كباقي شعوب العالم ـ تحولاً رقمياً أدى إلى الاعتماد على تكنولوجيا المعلومات والاتصالات وشبكة الإنترنت في كافة مجالات الحياة، وقد نتج عن الثورة الرقمية الحالية ظهور مجتمع المعلومات، وانتشار حقوق جديدة تُعرف بـ "الحقوق الرقمية"، والتي تعتبر ضرورية لا غنى عنها للحفاظ على الكرامة الإنسانية في مواجهة تهديدات العصر الرقمي. ولما كانت الشرطة هي الحامي الأول للحقوق والحريات العامة، فإنه يقع على عاتقها حماية حقوق الإنسان الرقمية وتعزيز احترامها في كافة المجالات، ومن بينها مجال العمل الأمني. إذ يشكل نقص الوعي لدى الكوادر الشرطية العربية بالحقوق الرقمية، وعدم اكتمال جاهزية الأجهزة الأمنية لمواجهة تحديات العصر الرقمي مشكلة البحث التي تمت مناقشتها وتحليلها، وأساساً لأهمية البحث وأهدافه وتساؤلاته وفرضياته ومنهجه.

وقد تم تقسيم الدراسة إلى ثلاثة مباحث؛ تناول المبحث الأول ماهية حقوق الإنسان الرقمية، موضحاً مفهومها ونطاقها وأنواعها؛ وذلك بعرض تعريفات المنظمات والهيئات الدولية، إضافة إلى بيان الأبعاد الاجتماعية والاقتصادية والسياسية للحقوق الرقمية، وإبراز أهمية إلمام الكوادر الشرطية العربية بهذه الحقوق الحديثة.

وناقش المبحث الثاني الانتهاكات والمخالفات الماسة بحقوق الإنسان الرقمية، حيث تم تحديد الانتهاكات المتعلقة بالجانب المالي لحقوق الإنسان الرقمية، وتلك المتعلقة بالجانب الأخلاقي، كما تناول المبحث مخالفات حقوق الإنسان الرقمية التي تُتهم الأجهزة الأمنية بارتكابها.

أما المبحث الثالث الخاص بدور أجهزة الشرطة في حماية وتعزيز حقوق الإنسان الرقمية، فقد تناول الأطر القانونية الدولية والوطنية المساندة لدور الشرطة في حماية حقوق الإنسان الرقمية، واشتمل على استعراض لجهود ومبادرات أجهزة الشرطة الدولية والإقليمية في حماية وتعزيز حقوق الإنسان الرقمية، كما تم تسليط الضوء على جهود أجهزة الشرطة العربية في هذا الجانب. وتم تعزيز الدراسة باستبيان حول وعي وجاهزية الكوادر الشرطية العربية للتعامل مع قضايا حقوق الإنسان الرقمية، بهدف تقديم نتائج واقعية تخدم العمل الشرطي.

وتوصلت الدراسة إلى نتائج هامة وقدمت توصيات قيمّة من شأنها المساهمة في تطوير جهود الأجهزة الأمنية العربية في هذا الجانب الحيوي.

الكلمات المفتاحية: حقوق الإنسان الرقمية، الشرطة الرقمية، الجرائم الرقمية، قوانين حقوق الإنسان، الدول العربية.

Digital Human Rights and Digital Police

Abstract:

Like other societies of the world, Arab societies have witnessed a digital transformation that has led to dependence on information and communication technology and the internet in all areas of life. Moreover, the digital revolution has resulted in the emergence of information society, and spread of new rights known as "digital rights", which are indispensable to preserving human dignity against threats of the digital age. Since police are the primary protector of public rights and freedoms, it is their responsibility to protect digital human rights and promote its respect in all fields, including the field of law enforcement. However, lack of digital rights awareness among Arab police forces and the incomplete readiness of security forces to face the challenges of the digital age, both constitute the research problem and the basis of its importance, objectives, questions and hypotheses.

The study was divided into three sections; the first dealt with the definition of digital human rights, explaining their meaning and scope by presenting the definitions of international organizations. In addition, it clarifies the social, economic and political dimensions of digital rights, and highlighting the importance of Arab police forces to be familiar with these modern rights.

The second section discussed the violations against digital human rights and determined those violations related to the financial and ethical aspects of digital rights. Also, it identified digital human rights violations that police forces are accused of committing.

As for the third section titled: the role of the police in protecting and promoting digital human rights, it dealt with international and national legal frameworks which support the function of police in protecting digital rights. Furthermore, it contained a review of the efforts and initiatives of international and regional police agencies in protecting and promoting digital human rights, besides the efforts of the Arab police forces in this aspect. Finally, the study was supported by a questionnaire on the awareness and readiness of Arab police forces to deal with digital human rights issues, with the aim of providing more realistic results that serve modernisation of police practices in the field.

Keywords: Digital human rights, digital police, digital crimes, human rights laws, Arab states.

قائمة الاختصارات:

Abbreviation الاختصار	Meaning in English المعنى باللغة الإنجليزية	Meaning in Arabic المعنى باللغة العربية
UDHR	Universal Declaration of Human Rights	**الإعلان العالمي لحقوق الإنسان**
ICESCR	International Covenant on Economic, Social and Cultural Rights	**العهد الدولي الخاص بالحقوق الاقتصادية والاجتماعية والثقافية**
ICCPR	International Covenant on Civil and Political Rights	**العهد الدولي الخاص بالحقوق المدنية والسياسية**
ECHR	European Convention on Human Rights	**الاتفاقية الأوروبية لحقوق الإنسان**
HRC	United Nations Human Rights Council	**مجلس حقوق الإنسان التابع للأمم المتحدة**
UNESCO	UN Educational, Scientific & Cultural Organization	**منظمة الأمم المتحدة للتربية والعلم والثقافة**
EU	Europe Union	**دول الاتحاد الأوروبي**
OSCE	Organization for Security and Co-operation in Europe	**منظمة الأمن والتعاون الأوروبية**
EDRI	European Digital Rights	**المنظمة الأوروبية للحقوق الرقمية**
EDRI-CDR	The Charter of Digital Rights	**ميثاق الحقوق الرقمية**
ENISA	EU Agency for Network & Info Security	**وكالة الاتحاد الأوروبي للأمن السيبراني**
AMNESTY	AMNESTY International	**منظمة العفو الدولية**
EUROPOL	EU Law Enforcement Agency	**وكالة تطبيق القانون الأوربية**
GCA	Global Cybersecurity Agenda	**البرنامج العالمي للأمن السيبراني**
GCI	Global Cybersecurity Index	**الدليل العالمي للأمن السيبراني**
IGF	the Internet Governance Forum	**منتدى الأمم المتحدة لحوكمة الإنترنت**
HRW	Human Rights Watch	**منظمة هيومن رايتس ووتش**
ICT	Information & Communication Technology	**تكنولوجيا المعلومات والاتصالات**
IMF	International Money Fund	**صندوق النقد الدولي**
INTERPOL	International Criminal Police Organization	**المنظمة الدولية للشرطة الجنائية**
ITU	International Telecommunication Union	**الاتحاد الدولي للاتصالات**
OHCHR	Code of Conduct for Law Enforcement Officials	**مدونة قواعد سلوك الموظفين المكلفين بإنفاذ القوانين**
NIST	National Institute of Standards &Technology	**المعهد الوطني للمعايير والتكنولوجيا**
OECD	Organization for Economic Co-operation and Development	**منظمة التعاون الاقتصادي للتنمية**
UNODC	UN Office on Drugs and Crime	**مكتب الأمم المتحدة المعني بالمخدرات والجريمة**
UNTOC	UN Convention Against Organized Crime	**اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة**
WEF	World Economic Forum	**المنتدى الاقتصادي العالمي**
WSIS	World Summit on the Information Society	**القمة العالمية لمجتمع المعلومات**

مقدمة:

باتت معالجة قضايا حقوق الإنسان في العمل الأمني أكثر تعقيداً وأكثر إلحاحاً من أي وقت مضى، ففي حين يقع على عاتق الأجهزة الأمنية مواجهة الإضطرابات والأزمات والكوارث ومكافحة الإرهاب والجريمة المنظمة والمخدرات التي تقتضي الاستعانة بتكنولوجيات المراقبة والتحقيق، تتسع دائرة "حقوق الإنسان" في عالم التكنولوجيا الرقمية وتعلو أصوات المنظمات الدولية لمضاعفة الحماية للكرامة الإنسانية والاستقلالية والخصوصية. وتُعتبر المعايير الدولية السارية في مجال حقوق الإنسان بمثابة ضمانات قانونية عالمية لحماية الأفراد من الاعتداءات التي تمس بالحريات الأساسية، وتُوصف "حقوق الإنسان الرقمية" Human Rights Digital بأنها حقوق تمكينية أساسية للحق في الكرامة والسلامة والحرية والتنمية الشخصية في مجتمع المعلومات أو العصر الرقمي (قرار الجمعية العامة للأمم المتحدة رقم ٧٢/٥٤٠ بشأن الحق في الخصوصية الرقمية)، وبالتالي ارتباط هذه الحقوق الأساسية بالأمن والنظام العام الذين تسهر أجهزة الشرطة على حمايتهما وتعزيزهما بكافة الإمكانيات المتاحة، ووفقاً للتشريعات النافذة، بغض النظر عن التحديات الرقمية الماثلة.

فلم تعد المجتمعات البشرية ـ ومن بينها المجتمعات العربية ـ هي ذاتها المجتمعات التي كانت تعيش زمن التكنولوجيا التناظرية في العقود الأولى من القرن العشرين، وإنما تغيرت وباتت تعيش اليوم عصر التكنولوجيا الرقمية، حيث تنتج أنشطتنا الرقمية على الأجهزة الإلكترونية المزودة بأجهزة استشعار كالحواسيب الشخصية والهواتف والساعات الذكية كل يوم حوالي ٢,٥ كوينتيليون بايت من البيانات القادرة على كشف السمات الشخصية وتحديد هوية كل فرد (bigdata technologies). فعلى الرغم من أن العصر الرقمي قد وفر الكثير من الخدمات الجليلة للبشرية، إلا أنه في نفس الوقت تتسارع وتيرة التهديدات الرقمية وانتهاكات حقوق الإنسان على شبكة الإنترنت، بأساليب لم يكن بالإمكان تصورها عندما صيغ الإعلان العالمي لحقوق الإنسان لعام ١٩٤٨ والعهدين الدوليين لعام ١٩٦٦.

وتشير الإحصائيات العالمية الأخيرة إلى أن عدد سكان العالم في بداية يناير ٢٠٢١ بلغ ٧,٨٣ مليار نسمة، بزيادة ٨٠ مليون عن عام ٢٠٢٠، فيما وصل عدد مستخدمي الإنترنت حول العالم أكثر من ٤,٦٦ مليار، أي بزيادة قدرها ٣٦٠ مليون مقارنةً بعام ٢٠٢٠، وتشكل هذه الزيادة ما نسبته ٥٩,٥٪ من عدد سكان العالم (Digital 2021: Global Overview Report). وعلى مستوى العالم العربي، بلغ عدد السكان في نهاية مارس ٢٠٢١ ما مجموعه ٤٢٣ مليون نسمة، وعدد مستخدمي الإنترنت حوالي ٣١٦ مليون، أي بنسبة ٧٤,٩٪ من عدد السكان، وبنسبة نمو بلغت ٥,٩٪ (internet world stats, 2021). ففي جمهورية مصر العربية على سبيل المثال، بلغ عدد السكان ١٠٣,٣ مليون نسمة، وعدد مستخدمي الإنترنت ٥٩,١٩ مليون، بنسبة ٥٧,٣٪ من عدد السكان، لتحتل بذلك المرتبة (١٩) في الترتيب العالمي. وفي المملكة المغربية بلغ عدد السكان ٣٧,١٣ مليون، وعدد مستخدمي الإنترنت ٢٧,٦٢ مليون، بنسبة ٧٤,٧٪ من عدد السكان،

لتحتل بذلك المرتبة (٣٢) عالمياً. وفي المملكة العربية السعودية بلغ عدد السكان ٣٥,٠٨ مليون، وعدد مستخدمي الإنترنت ٣٣,٥٨ مليون، بنسبة ٩٥,٧٪ من عدد السكان، وبترتيب عالمي رقم (٢٩). وأخيراً، في دولة قطر بلغ عدد السكان ٢,٩١ مليون، وعدد مستخدمي الإنترنت ٢,٨٨ مليون، بنسبة ٩٨,٩٦٪ من نسبة عدد السكان، وبترتيب عالمي رقم (١٤) (Statista, 2021).

وكنتيجة لهذا التحول الرقمي، ودخول تكنولوجيا المعلومات والاتصالات في أدق تفاصيل الحياة الشخصية، وتغلغلها في جميع مناحي الحياة والمعاملات المدنية والتجارية والمصرفية والصحية والتعليمية، برزت حقوق الإنسان الرقمية كأحد أهم الحقوق المعاصرة لضمان الكرامة الإنسانية والأمن والخصوصية في الفضاء الرقمي. فربما لا يستطيع الإنسان أن يعزل نفسه عن استخدام الأجهزة الحاسوبية وشبكة الإنترنت والحكومة الإلكترونية وغيرها من الخدمات الرقمية، ولكن بالتأكيد له الحق في أن تُحترم خصوصياته وشؤون أسرته وحرياته الأساسية. ولقد فجّرت المقولة الشهيرة: "لا أريد أعيش في عالم يسجّل فيه كل ما أقوم به وكل ما أقوله" نقاشاً محتدماً في الجمعية العامة للأمم المتحدة والمنظمات الدولية المختصة، حيث صرح الأمين العام للأمم المتحدة بأن مدى تأثير التكنولوجيا الرقمية على مستوى الأمن والأمان في المجتمعات مرتبط بقدرة الأجهزة الأمنية وبالشراكة مع الجهات المختصة على الحد من انتهاكات حقوق الإنسان الرقمية على شبكة الإنترنت وتعزيز استخداماتها الشرعية (UN, Road map for digital cooperation, 2020).

من المعلوم أن الشرطة هي الساهر على حماية القانون والنظام، وهي صمام الأمان في الدفاع عن حقوق الإنسان، إلا أن أجهزة الشرطة العربية كانت تعمل خلال العقود الماضية على بناء قدراتها في حماية حقوق الإنسان التقليدية ومكافحة الجرائم الواقعة على الحق في الحياة والسلامة الجسدية، ولكن هذه الجرائم أضحت اليوم بعيدة كل البعد عن أن تشكل التحدي الأمني الوحيد، فقد نتج عن هيمنة الفضاء الرقمي ظهور تحديات إجرامية جديدة تستهدف طائفة حديثة من حقوق الإنسان، تُعرف بالحقوق الرقمية. حيث تشير الإحصائيات في عام ٢٠١٩ إلى أنه تم تسجيل أكثر من ٧٠٠٠ عملية اختراق للبيانات، أدت إلى الكشف عن أكثر من ١٥ بليون سجل (Risk Based Security Report, 2019)، ناهيك عن الاعتداءات الرقمية الأخرى المرتبطة بقضاء الأفراد أوقاتاً على الإنترنت كالاحتيال وسرقة البيانات والتحرش أو الاستغلال الجنسي للأطفال.

يبدو واضحاً بأن تغلغل وإتساع الفضاء الرقمي قد فرض تحدٍ واقعياً جديداً على واجبات الشرطة التقليدية، الأمر الذي يحتم بناء وتطوير سياسات وقدرات رقمية جديدة، قادرة على مواكبة المتغيرات المجتمعية وحماية حقوق الإنسان في العصر الرقمي. ومن أبرز المفاهيم المستحدثة المرتبطة بحماية حقوق الإنسان في مجتمع المعلومات، تبني تقنيات الشرطة الرقمية Digital Police، مما يقتضي تقييم مدى استعداد وجاهزية أجهزة الشرطة العربية للتعامل مع قضايا حقوق الإنسان الرقمية ومواجهة التحديات الرقمية المستقبلية ذات العلاقة.

مشكلة البحث:

إن ضابط الشرطة الباحث في مجالات حقوق الإنسان يكون في الغالب واقعاً بين حملين ثقيلين؛ وهما إما الإنتصار للوظيفة الأمنية، أو الإنتصار لحقوق الإنسان وحرياته الأساسية. والواقع أن حماية الأمن وضمان احترام حقوق الإنسان هما واجبين متلازمين يقعا على عاتق رجال الشرطة، فحماية حقوق الإنسان جزءٌ من حماية الأمن الوطني، ويفترض في التدابير الأمنية السعي دوماً لتعزيز حقوق الإنسان. إلا أن التطورات الناجمة عن العصر الرقمي، كما أفرزت حقوق وحريات جديدة، فإنها أيضاً أتاحت وسائل وتقنيات قد يؤدي إساءة استخدامها إلى انتهاك حقوق الإنسان الرقمية، وتنسب بعض التقارير ــ التي سيتم مناقشتها لاحقاً ــ بعض هذه الانتهاكات لمنتسبي الأجهزة الأمنية.

وتكمن مشكلة البحث في ضعف وعي الكوادر الشرطية العربية بالممارسات والآثار السلبية والخطيرة لسوء إستغلال تكنولوجيا المعلومات والاتصالات على الحقوق والحريات في البيئة الرقمية، حيث تنتهك الاختراقات والاعتداءات على الحواسيب الشخصية والهواتف الذكية ومواقع التواصل الاجتماعي حقوق الأفراد في السلامة والكرامة وسرية بياناتهم الخاصة، مما يجعل حاجة الأجهزة الأمنية لبناء قدراتها الرقمية كبيرة وماسة، إذ يعتبر وعي رجل الأمن بهذه الحقوق والتهديدات حجر الأساس الذي تنبني عليه سبل المواجهة اللاحقة. فإذا كان يقع على عاتق الكوادر الأمنية حماية المنجزات الرقمية التي سعت الدول العربية إلى تحقيقها طوال العقد الماضي ٢٠١٠- ٢٠٢٠ بالتوجه نحو رقمنة البيانات والمعلومات والمعاملات وتطبيق أنظمة الحكومة الإلكترونية سعياً لتطوير مجتمعاتها، فإن تنمية المقدرات والمهارات الشرطية والأمنية لا ينبغي إغفالها. وتتضمن معالجة مشكلة البحث أيضاً تأطير الأبعاد الاجتماعية والاقتصادية والسياسية لحقوق الإنسان الرقمية، ومن جانب آخر الرؤى الاستراتيجية والآفاق المستقبلية لأنظمة عمل الشرطة الرقمية التي تكفل التعايش مع التكنولوجيات الجديدة.

أهمية البحث:

يستقي البحث أهميته في الوقت الراهن من الأهمية المتنامية لحقوق الإنسان الرقمية، ومن خطورة الأوضاع الراهنة والتهديدات الرقمية المحدقة بالمنطقة، إذ تُجمع التقارير المتخصصة على تصاعد حجم الاعتداءات الرقمية عالمياً وازدياد مخاطر البرمجيات الخبيثة وممارسات التجسس والتصيد الإلكتروني على الأفراد والمؤسسات حول العالم، وفي الدول العربية بصفة خاصة، حيث التغيرات السياسية والاقتصادية، وحداثة استخدام وتطبيق أنظمة تقنية المعلومات والحكومة الإلكترونية والتجارة الإلكترونية وغيرها من الاستثمارات الرقمية، مما يجعل المنطقة بيئة جاذبة للإجرام الرقمي، ويستوجب بالتالي مضاعفة وعي الأجهزة الأمنية وتطوير الآليات التشريعية والتقنية للوقاية وتحقيق المستوى المنشود من الاحترام لحقوق الإنسان الرقمية، بما يعزز أمن واستقرار الشعوب العربية ويخدم تطلعات حكوماتها باستثمار التطبيقات التكنولوجيات الرقمية.

أهداف البحث:

أرست خارطة طريق الأمم المتحدة لحماية حقوق الإنسان الرقمية لعام ٢٠٢٠ سبعة أهداف استراتيجية لتعزيز احترام حقوق الإنسان في العصر الرقمي، وفي نهج مشابه، ولكن بطموحات عربية كبيرة، يسعى هذا البحث المتخصص إلى تحقيق الأهداف التالية:

١. إبراز مفهوم حقوق الإنسان الرقمية وأهميتها وأبعادها على المستويين الدولي ومستوى الدول العربية.
٢. تقديم صورة واقعية وشاملة عن أخطر الانتهاكات التي تتعرض لها حقوق الإنسان الرقمية على الصعيدين الدولي والعربي.
٣. رفع وعي وإدراك الكوادر الشرطية العربية بقضايا حقوق الإنسان الرقمية في العمل الأمني المعاصر.
٤. التعرف على أحدث الصكوك الدولية والتشريعات الوطنية ذات الصلة بحقوق الإنسان الرقمية.
٥. عرض التجارب والخبرات الدولية والإقليمية الرائدة في مجال حماية حقوق الإنسان الرقمية والشرطة الرقمية وكيفية الاستفادة منها.
٦. إبراز المبادرات العربية لتعزيز مفاهيم حقوق الإنسان الرقمية في العمل الأمني ومدى نجاحها.
٧. الوقوف على مدى استعداد وجاهزية أجهزة الشرطة العربية لمواكبة التحولات الرقمية والتعامل مع التحديات المعاصرة بشأن حقوق الإنسان الرقمية.
٨. مناقشة تقنيات وتطبيقات الشرطة الرقمية ودورها في تعزيز مفاهيم وقيّم حقوق الإنسان الرقمية.
٩. تقديم مقترحات مستمدة من أحدث المعايير الدولية من شأنها المساهمة في بناء وتطوير ودعم جهود أجهزة الشرطة العربية لحماية وتعزيز حقوق الإنسان الرقمية.

فرضيات البحث:

- وضوح مفهوم ونطاق حقوق الإنسان الرقمية يشكل القاعدة الأساسية لآليات الحماية القانونية والأمنية.
- تأكيد أهمية وأبعاد حقوق الإنسان الرقمية يحفز الجهات الأمنية لاتخاذ تدابير الحماية اللازمة.
- تحقيق التوازن والمواءمة بين متطلبات الأمن الوطني واحترام حقوق الإنسان الرقمية متيسر متى ما توافر الوعي والتدريب الشرطي الملائم.
- فعالية التدابير الأمنية في مواجهة الانتهاكات الماسة بحقوق الإنسان الرقمية مرتبطة ارتباطاً كبيراً بفعالية الأطر التشريعية والسياسات التنظيمية.
- تطبيق أسس ومعايير الشرطة الرقمية أصبح ضرورة لمواكبة التحول المجتمعي الرقمي.

تساؤلات البحث:

لدراسة ومعالجة التحديات المتعلقة بقضايا حقوق الإنسان الرقمية في العمل الأمني العربي، يناقش البحث

التساؤلات التالية:

- ما هو مفهوم حقوق الإنسان الرقمية؟ وما هي أنواعها؟ وبماذا تختلف عن حقوق الإنسان التقليدية؟
- ما هي أهمية حقوق الإنسان الرقمية؟ وما هي أبعادها الأمنية؟
- ما هي المتطلبات الأمنية لمجتمع المعلومات في العصر الرقمي؟ وما مدى أهمية إلمام الكوادر الشرطية العربية بحقوق الإنسان الرقمية؟
- ما هي أبرز الانتهاكات والمخالفات الماسة بحقوق الإنسان الرقمية؟
- ما هو الدور المأمول لأجهزة الشرطة العربية في حماية وتعزيز حقوق الإنسان الرقمية؟
- ما هي أفضل التجارب والممارسات الشرطية الدولية والإقليمية في حماية الحقوق الرقمية ومواكبة العصر الرقمي؟
- ما مدى استعداد وجاهزية أجهزة الشرطة العربية لمواجهة متطلبات وتحديات التكنولوجيات الرقمية؟
- ما مدى حاجة الدول العربية لاعتماد استراتيجيات رقمية ومدونات سلوك موحدة للأجهزة الأمنية تراعي الالتزام بحقوق الإنسان الرقمية؟

حدود البحث:

تتسم حقوق الإنسان عموماً بعالمية النطاق وشمولية المدى؛ أي أنها تشمل كافة أفراد المجتمع الدولي وتحيط بكافة المصالح الإنسانية الأساسية، إلا أن حقوق الإنسان الرقمية أضافت حقوقاً جديدة مرتبطة بالفضاء الرقمي، الأوسع نطاقاً والعابر للحدود والقارات، مما يقتضي مناقشة أنواعها وأبعادها ومهدداتها عالمياً، والتعرف على الجهود الدولية والإقليمية لحمايتها. غير أن الحدود الموضوعية للبحث يحدد إطارها موضوع المسابقة المُختار، وهو "حقوق الإنسان الرقمية"، وعليه فقد انطلق هذا البحث من رؤية حدد معالمها مجلس وزراء الداخلية العرب، الذي أخذ على عاتقته مهمة نشر الوعي بقضايا حقوق الإنسان في العمل الأمني، والحاجة إلى التعاون في معالجتها وتعزيزها على مستوى مراكز القرار العربي.

الدراسات السابقة:

بالرغم من حداثة موضوع البحث وندرة مراجعه، إلا أن البحث يستند على عدد من الدراسات والتقارير الحديثة الصادرة من المراكز الدولية والعلمية المتخصصة، والتي سيتم الاستفادة من تجاربها ونتائجها في إثراء البحث، وفيما يلي استعراض لنماذج محدودة منها:

Wagner, Kettemann & Vieth. 2019. *Research Handbook on Human Rights and Digital Technology*, Elgar

تميزت هذه الدراسة الأكاديمية المعمقة بشمولية محاورها التي غطت عشرون موضوعاً في مجال حقوق الإنسان والتكنولوجيا الرقمية؛ وذلك إبتداءً من بيان طبيعة حقوق الإنسان في الفضاء الرقمي، وتهديدات حقوق الإنسان على الإنترنت، وصولاً إلى الأمن الرقمي وحقوق الإنسان الأساسية، وإنتهاءً بمستقبل حقوق الإنسان الرقمية. وقد ناقشت الدراسة باستفاضة سؤال محوري وهو السبل المثلى لحماية حقوق الإنسان الرقمية، وخلصت إلى هناك حاجة ملحة لضمان دمج مبادئ حقوق الإنسان بشكل منهجي في صميم سياسات تطوير التكنولوجيا الرقمية وحوكمة الإنترنت والتشريعات المنظمة، وبخلاف ذلك فإن هذه الحقوق معرضة للتلاشي تدريجياً. وبالرغم من العمق الدولي والتقني للدراسة، إلا أنها لم تتعرض بشكلٍ كافٍ للمجالين الأمني والقانوني.

UN Human Rights Council. 2020. *Impact of New Technologies on The Promotion and Protection of Human Rights*, (A/HRC/44/24)

ركزت مفوضية الأمم المتحدة لحقوق الإنسان في هذا التقرير ـ الذي يمثل دراسة متخصصة في أثر التكنولوجيات الجديدة على حماية حقوق الإنسان ـ على موضوع محدد، وهو عدم شرعية استخدام تكنولوجيا المعلومات والاتصالات في تعطيل المنصات الرقمية التي تدعو لتنظيم تجمعات سلمية ومراقبة المتظاهرين وقمع ممارسة الحقوق الرقمية الأخرى. وتتجلى فائدة الدراسة في استعراضها لمختلف التكنولوجيات الحديثة المستخدمة في انتهاك حقوق الإنسان الرقمية وموقف القانون الدولي منها، حيث أكدت بأن عمليات الأغلاق العام للإنترنت تمثل إخلالاً بالتزامات الدول باحترام مجموعة واسعة من الحقوق الرقمية. وتتوقع الدراسة بتزايد هذه الممارسات بتزايد الاحتجاجات، إلا أنها لم تقدم حلولاً عملية وقانونية ملائمة لمواجهتها.

National Institute for Advanced Studies in Security & Justice. 2018. *Digital Transformations in Policing To 2025: Anticipation & Performance*

هدفت هذه الدراسة إلى مناقشة تأثيرات الثورة الرقمية الحالية على العمل الشرطي والأمني؛ بمعنى كيف يمكن للأجهزة الأمنية الاستفادة من تقنيات البيانات الضخمة، وإنترنت الأشياء، وجمع المعلومات الرقمية، والمراقبة الذكية عبر الإنترنت، وغيرها الكثير من التكنولوجيات الرقمية، التي باتت تفرض على أجهزة الشرطة تطوير حضور جديد لها على الإنترنت والدخول في عصر جديد من الاتصالات. وتوصلت هذه الدراسة إلى أنه في حين سارعت المنظمات الإجرامية إلى اغتنام الفرص التي أتاحتها الثورة الرقمية في ارتكاب جرائم الإنترنت المنظمة، لا زالت أجهزة الشرطة في العالم تفتقر إلى رؤية واضحة في هذا المجال. وبينما ترسم هذه الدراسة تصوراً مستقبلياً للشرطة الرقمية بفعل التطورات التكنولوجية، إلا أن محاذير ومعوقات التحول الأمني الرقمي ـ خصوصاً بالنسبة للعالم العربي ـ لم تكن واضحة في هذا السياق.

منهج البحث:

بالنظر إلى الطبيعة القانونية للبحث والأهداف الأمنية التي يسعى لتحقيقها، سيتم الاستعانة بالمنهج الوصفي التحليلي، فباعتبار أن حقوق الإنسان منظمة وفق قواعد قانونية وإجرائية، سيتم استخدام المنهج الوصفي لتوضيح الأطر القانونية الدولية والوطنية المتعلقة بحقوق الإنسان. كما سيتم الاستعانة بالمنهج التحليلي لمناقشة وتحليل واقع حقوق الإنسان الرقمية في الدول العربية من حيث التشريعات والقواعد التنظيمية والإجرائية، وصولاً لاستخلاص وتحديد المخاطر والتهديدات الرقمية وما يقابلها من جهود ومبادرات. كما أنه بهدف إضفاء عمق وطابع عملي يعكس الطبيعة الواقعية لحقوق الإنسان الرقمية، تم تدعيم البحث باستبانة (ملحقة) للوقوف على آراء رجال الشرطة حول بعض القضايا الهامة التي تثيرها حقوق الإنسان الرقمية في العمل الأمني، ومدى مواكبة المؤسسات الأمنية للتطورات والتحديات الرقمية.

خطة البحث: تم تقسيم الدراسة إلى ثلاثة مباحث رئيسية، كما يلي:

المبحث الأول: ماهية حقوق الإنسان الرقمية

المطلب الأول: مفهوم ونطاق حقوق الإنسان الرقمية

المطلب الثاني: الأبعاد الاجتماعية والاقتصادية والسياسية لحقوق الإنسان الرقمية

المطلب الثالث: أهميـة إلمام الكوادر الشرطية العربية بحقوق الإنسان الرقمية

المبحث الثاني: الانتهاكات والمخالفات الماسة بحقوق الإنسان الرقمية

المطلب الأول: الانتهاكات المتعلقة بالجانب المالي لحقوق الإنسان الرقمية

المطلب الثاني: الانتهاكات المتعلقة بالجانب الأخلاقي لحقوق الإنسان الرقمية

المطلب الثالث: مخالفات حقوق الإنسان الرقمية التي تُتهم الأجهزة الأمنية بارتكابها

المبحث الثالث: دور أجهزة الشرطة في حماية وتعزيز حقوق الإنسان الرقمية

المطلب الأول: الأطر القانونية الدولية والوطنية المساندة لدور الشرطة في حماية حقوق الإنسان الرقمية

المطلب الثاني: جهود ومبادرات أجهزة الشرطة الدولية والإقليمية في حماية وتعزيز حقوق الإنسان الرقمية

المطلب الثالث: جهود أجهزة الشرطة العربية في حماية وتعزيز حقوق الإنسان الرقمية

المطلب الرابع: نتائج استبيان قياس وعي وجاهزية الكوادر الشرطية العربية للتعامل مع قضايا حقوق الإنسان الرقمية

الخاتمة: وتتضمن مجموعة من النتائج والتوصيات.

المبحث الأول
ماهية حقوق الإنسان الرقمية

تمهيد وتقسيم:

يعيش العالم حالياً ثورة تكنولوجية وطفرة تقنية أدت إلى رقمنة البيانات وحوسبة الكثير من المعلومات، بحيث أتاحت التكنولوجيات الرقمية الحديثة وسائل جديدة لممارسة حقوق الإنسان، بالإضافة إلى ارتباط معظم البنى التحتية والخدمات المجتمعية الأساسية كالغذاء والطاقة والنقل والاتصالات بشبكة الإنترنت وبرمجيات الحاسوب، مما أدى إلى ظهور طائفة جديدة من حقوق الإنسان تُعرف بالحقوق الرقمية (digital rights)، لذلك أصبحت حقوق الإنسان الرقمية (digital human rights) من الركائز الحيوية التي تكتسب أهمية متزايدة بسبب أهمية تكنولوجيا المعلومات وسيادة الإنترنت من جانب، وتنامي المخاطر والتهديدات الرقمية من جانب آخر؛ فمع كل انتهاك أو اختراق إلكتروني مؤثر، تبرز الحاجة إلى وسائل أمن إلكترونية وقدرات شرطية رقمية تكفل حماية البيئة الإلكترونية الوطنية وحقوق الإنسان الرقمية.

ويمكن القول بأن أولى خطوات الحماية الأمنية الفعالة تبدأ من تحديد العناصر المشمولة بالحماية تحديداً دقيقاً، إذ بات مصطلح " حقوق الإنسان الرقمية " محل بحث واهتمام عدة منظمات دولية وتشريعات وطنية، نظراً لما يُمثله من أهمية استراتيجية لمجتمع المعلومات ومنظومة الأمن الوطني الشامل. بناءً عليه، يسعى هذا المبحث إلى بيان مفهوم ونطاق حقوق الإنسان الرقمية، وأبعادها الاجتماعية والاقتصادية والسياسية، وصولاً إلى أهمية إلمام منتسبي الأجهزة الأمنية العربية بها، كلاً في مطلب مستقل.

المطلب الأول
مفهوم ونطاق حقوق الإنسان الرقمية

بعد مُضي أكثر من سبعون عاماً على صدور الإعلان العالمي لحقوق الإنسان (UDHR 1948)، شهدت حقوق الإنسان الأساسية التي أقرتها هذه الوثيقة الأممية التاريخية (كالحق في الحياة والحرّية والأمان والمساواة والجنسية والتنقل والإقامة والتعليم والصحة والتملُّك والعمل والتجمع) درجة كبيرة من الوضوح والرسوخ في ضمير البشرية، بل وقدرٍ مساوٍ كذلك من الاحترام والحماية من قبل دساتير وحكومات دول العالم بما يخدم تطلعات وكرامة شعوبها. ولعل مما ساهم في استقرار حقوق الإنسان وحرياته الأساسية واحترامها على المستويين العالمي والإقليمي هو صدور أكثر من سبعين معاهدة لحماية حقوق الإنسان HR Conventions يجري تطبيقها اليوم على أساس ثابت ودائم.

في المقابل، ونظراً لحداثتها، لم تحظ حقوق الإنسان الرقمية بذات القدر من الوضوح والتحديد، وذلك بالرغم من أهميتها الأمنية والاجتماعية المتصاعدة، وقد يكون هذا الغموض راجعاً إلى الطبيعة العالمية والتقنية

للحقوق الرقمية وتطورها مع التحولات التكنولوجية، فهي كما يصفها قرار الجمعية العامة للأمم المتحدة رقم (٦٤/٢١١) بشأن أمن الفضاء الإلكتروني (UNGA Resolution) أحد أهم المسائل والتحديات الكبرى؛ إذ تتعرض حقوق الإنسان الرقمية على الإنترنت ـ كما سيتم بيانه ـ لاعتداءات كثيرة. كما أنه بخلاف حقوق الإنسان الأساسية، لم تصدر حتى الآن وثيقة أممية محددة ومستقلة بشأن الحقوق الرقمية أو "حقوق الإنترنت" أو "حقوق المعلوماتية" كما يسميها البعض (UNESCO, 2015).

وبحكم البُعد الدولي والإنساني للحقوق الرقمية، تُعد التقارير الدولية الصادرة عن المنظمات والهيئات الدولية المتخصصة بمثابة مرجعيات أساسية موثوقة يمكن الاستناد إليها للوصول إلى فهم دقيق وشامل للحقوق محل البحث وموضوع الحماية. وفي هذا المجال، وإنطلاقاً من اختصاصه الأصيل في وضع المعايير التقنية التي تضمن سلامة وسلاسة تشغيل شبكات تكنولوجيا المعلومات والاتصالات حول العالم، أشار الاتحاد الدولي للاتصالات ITU إلى مسؤولية الدول في بناء الثقة والأمان عند استخدام تقنيات الاتصال الجديدة ومنع أي انتهاك لحقوق الإنسان الرقمية (ITU, Guidelines for Utilization of the GCA, 2021)، إلا أنه لم يقدم تعريفاً مفصلاً للمصطلح، ولعل ذلك بسبب الطبيعة التقنية الصرفة لهذه المنظمة.

بينما وصفت منظمة الأمم المتحدة للتربية والعلم والثقافة UNESCO حقوق الإنسان الرقمية بأنها تشمل حق الوصول إلى المعلومات والمعرفة، وحق التعلم الإلكتروني والعلوم الإلكترونية، وحق التنوع الثقافي واللغوي، وحق الإطلاع على الصحافة والإعلام (UNESCO, Keystones to Foster Inclusive Knowledge Societies, 2015). أما منظمة الأمن والتعاون الأوروبية OSCE، فقد حصرت الحقوق الرقمية في حق الإنسان في حرية التعبير على الإنترنت، مع التركيز على سلامة الصحفيين وحرية المحتوى الصحفي عبر الإنترنت (OSCE, Freedom of the Media, 2016).

وبمراجعة التقارير الصادرة عن القمة العالمية لمجتمع المعلومات WSIS، تبين استخدامها لعدة مصطلحات في هذا الشأن؛ كـ "حقوق الإنترنت" internet rights، و "حقوق الإنسان على الإنترنت" human rights online، و "الحقوق الرقمية" digital rights، إلا أن جميع هذه المصطلحات استخدمت بشكل مترادف للإشارة تحديداً إلى الحق في حرية التعبير عن الرأي، والحق في الخصوصية، والحق في حماية البيانات الخاصة (WSIS, (Tunis Agenda for the Information Society, 2005. وقد تبنى مجلس حقوق الإنسان التابع للأمم المتحدة HRC نتائج أعمال هذه القمة، وأكد بأن حقوق الإنسان في مجتمع المعلومات باتت تفوق المفهوم التقليدي لحقوق الإنسان، لتشمل طائفة أوسع من الحقوق الرقمية التي توفرها التكنولوجيات الرقمية لكافة الأقطار والأجناس والأعمار (HRC, Right to Privacy, 2016).

وفي تطور هام، قدمت المنظمة الأوروبية للحقوق الرقمية EDRI ميثاقاً خاصاً بالحقوق والحريات الرقمية، ينص على جملة من الحقوق الرقمية أبرزها: الحق في الخصوصية، والحق في إخفاء الهوية والسرية، والحق في النفاذ إلى التكنولوجيا والمعرفة، والحق في تشفير البيانات (EDRI, The Charter of Digital Rights ,2014). وبالرغم من الطبيعة الاسترشادية غير الإلزامية لهذا الميثاق، إلا أنه شكل عامل ضغط أخلاقي على حكومات الدول، وفق ما أشار منتدى الأمم المتحدة لحوكمة الإنترنت IGF المنعقد في برلين في عام ٢٠١٩ (Fourteenth Annual Meeting of the Internet Governance Forum)، والذي أكد بدوره على ارتباط حقوق الإنسان الرقمية بالرفاه والتنمية الاجتماعية وسلامة الأفراد في المجتمع الرقمي.

ومن الوثائق الرسمية الأبرز في هذا المجال، "ميثاق الحقوق الرقمية الأساسية للاتحاد الأوروبي" الذي تولى مراجعته في عام ٢٠١٨ مجموعة من الخبراء الحكوميين والأكاديميين في مجال حقوق والإنسان والأمن الرقمي، حيث نص الميثاق في ديباجته على ضرورة تسخير التقدم التقني لخدمة الإنسانية واحترام حقوق الإنسان في العالم الرقمي، ومن ثم أورد عشرة حقوق رقمية باعتبارها حقوقاً أساسية، وهي: ١- الحق في التمتع بالسلامة والكرامة لاسيما ضد تقنيات الذكاء الاصطناعي والبيانات الضخمة والتعلم الآلي والروبوتات؛ ٢- الحق في حرية التعبير والاتصال؛ ٣- الحق في الوصول للمعلومات والمعارف؛ ٤- الحق في النفاذ إلى البيئة الرقمية على قدم المساواة دون حظر أو تمييز؛ ٥- الحق في احترام الحياة الخاصة؛ ٦- الحق في الخصوصية وسرية البيانات الشخصية؛ ٧- الحق في تشفير البيانات الخاصة؛ ٨- الحق في التمتع بشبكة رقمية آمنة ومستديمة؛ ٩-الحق في استخدام أجهزة إلكترونية وبرمجيات وترددات لاسلكية خالية من القيود؛ ١٠- الحق في إنشاء مواقع إلكترونية على الويب (Charter of Digital Fundamental Rights of the European Union). وهو ما يبين وبشكل جلي المفهوم العام والنطاق النوعي لحقوق الإنسان الرقمية.

وعلى الرغم من عدم تطرق "الميثاق العربي لحقوق الإنسان" المعدل سنة ٢٠٠٤م لتعريف حقوق الإنسان الرقمية بشكل صريح، إلا أن الميثاق يؤكد في ديباجته على حق الإنسان في التمتع بالحرية والعدل والمساواة. كما ينص الميثاق في المادة (٣٢) على "الحق في الإعلام وحرية الرأي والتعبير"، وهو ما ينسجم مع القانون الدولي الإنساني، ويتماشى مع ما أقرته المعاهدات الدولية لحقوق الإنسان بضرورة حماية حرمة الحياة الخاصة وسرية المراسلات وغيرها من وسائل الاتصالات الخاصة. إلا أن هذا التوافق العام لا يعفي الميثاق العربي من التعديل والارتقاء إلى مستوى الحقوق الرقمية الصريحة الواردة في الوثائق الدولية لحقوق الإنسان، كالميثاق الأوروبي للحقوق الرقمية السابق الإشارة إليه، وذلك بما يواكب التطورات الرقمية في العالم العربي.

ويرى جانب من الفقه العربي بأن مفهوم الحقوق الرقمية ينصرف إلى حماية كافة حقوق الإنسان وحرياته الأساسية في البيئة الرقمية، فالحقوق الرقمية وفقاً لهذا الرأي هي ذات حقوق الإنسان التقليدية ولكن تتم

ممارستها عبر الوسائط الرقمية (د. عبديش، ٢٠٢٠م). كما تُصور بعض الكتابات العربية تعلق مصطلح الحقوق الرقمية بحماية حقوق الإنسان المعروفة كالحق في حرية التعبير والحق في سرية البيانات الخاصة عندما تجري ممارستها بواسطة التقنيات الرقمية الجديدة (جناحي، ٢٠١٨م). ويبدو هذا القول مستمداً من البيان الوارد بقرار مجلس حقوق الإنسان التابع للأمم المتحدة رقم (٢٠/٨) لسنة ٢٠١٢م بأن "ذات الحقوق التي يتمتع بها الأشخاص خارج البيئة الرقمية [offline]، يجب أيضاً أن تخضع للحماية في البيئة الرقمية [online] ".

ولا يرى الباحث دقة هذا الرأي المُضيَّق لنطاق حقوق الإنسان الرقمية، لأن الحقوق الرقمية تشمل حقوقاً جديدة لم ترد صراحةً في الإعلان العالمي لحقوق الإنسان أو حقبة ما قبل العصر الرقمي؛ كالحق في حماية الهوية الرقمية وحق النفاذ إلى الإنترنت وحقوق المستخدم ضد شركات الإنترنت والحق في تشفير البيانات، وبالتالي تُعد إضافة لحقوق الإنسان الأساسية؛ أو بمعنى آخر، تُعد أشمل وأوسع نطاقاً من حقوق الإنسان، وإن كانت هذه الأخيرة هي الأساس والقاعدة للحقوق الرقمية. لذلك يرى بعض الفقه الغربي تقسيم حقوق الإنسان الرقمية إلى حقوق رقمية كلاسيكية classical digital rights وهي الحقوق الرقمية الأساسية كالحق في الخصوصية وحماية البيانات وحرية التعبير؛ وحقوق رقمية متطورة developed digital rights وتشمل كافة الحقوق أو المنافع الجديدة المنبثقة من التقنيات الرقمية وشبكة الإنترنت (Zalnieriute, 2019, 411). بمعنى أن نطاق حقوق الإنسان الرقمية في تطور مستمر استجابةً للتغيرات المجتمعية والتطورات التكنولوجية الجديدة. بناءً عليه، يرى Benedek بضرورة إعادة ضبط وتعديل حقوق الإنسان الأساسية لتتلاءم مع طبيعة البيئة الإلكترونية أو الرقمية، وذلك من خلال إعادة تفسير حقوق الإنسان القائمة، أو إنشاء حقوق إنسان جديدة، أو وضع قواعد تنظيمية جديدة تتناسب مع احتياجات الحماية القانونية الرقمية (Benedek, 2019, 364).

يتبين من خلال مناقشة وتحليل المفاهيم الدولية والفقهية لحقوق الإنسان الرقمية أن مضامينها ومدلولاتها تدور بشكل أساسي حول توفير حقوق ضرورية مستحدثة للإنسان في العصر الرقمي؛ إذ على غرار حقوق الإنسان في البيئة الواقعية، تستلزم البيئة الرقمية حقوق خاصة تضمن كرامة وسلامة الإنسان عند إبحاره في الشبكة العنكبوتية. ويمكن القول بأن التعاريف أو الأوصاف المتقدمة ـ في مجموعها ـ تسلك مسارين: يركز الأول على حقوق الإنسان في الاتصال المفتوح وغير المقيد بالإنترنت وخطوط الاتصالات والشبكات؛ ويركز الثاني على حرية وسرية التواصل وتداول البيانات عبر البيئة الرقمية وما يحيط بها. فحقوق الإنسان الرقمية في نهاية المطاف تغطي مجموعة واسعة من الحقوق المتعلقة بالإنترنت وما يتيحه من خدمات تمكن الأفراد من ممارسة حقوق اقتصادية واجتماعية وثقافية، مثل الحق في التعليم والصحة والمشاركة في الحياة الثقافية والتمتع بفوائد التقدم العلمي وتطبيقاته، وكذلك الحقوق المدنية والسياسية، مثل الحق في التجمع وحرية التعبير وتكوين الجمعيات، وبالتالي يعمل الإنترنت كوسيلة أساسية تتيح للأفراد ممارسة مجموعة أخرى من الحقوق الرقمية التي تقوم على أساس تعزيز الكرامة الإنسانية والاستفادة من التطورات التكنولوجية من أجل رفاهية الإنسان.

المطلب الثاني
الأبعاد الاجتماعية والاقتصادية والسياسية لحقوق الإنسان الرقمية

إذا كان العهد الدولي الخاص بالحقوق الاقتصادية والاجتماعية والثقافية (ICESCR) ، العهد الدولي الخاص بالحقوق المدنية والسياسية (ICCPR) الصادرين في عام ١٩٦٦ يدللان معاً ـ وبشكل جلي ـ على الأبعاد الاقتصادية والاجتماعية والثقافية والسياسية لحقوق الإنسان، فإن أبعاد حقوق الإنسان الرقمية وأهميتها الأمنية تحتاج للإيضاح والتحليل بسبب حداثة انتشارها وقلة التشريعات الوطنية الناظمة لها، حيث يؤكد George Christou ـ خبير الأمن الرقمي لدى الاتحاد الأوروبي ـ بأن حماية الحقوق الرقمية أصبح شرطاً أساسياً لحماية المصالح الاجتماعية والثقافية ولتعزيز النمو الاقتصادي (Christou, 2016). بناءً عليه، يسعى هذا المطلب إلى بيان الأبعاد المختلفة لحقوق الإنسان الرقمية، ذلك أن من شأن إيضاح هذه الأبعاد التأثير في مستوى الحماية القانونية والأمنية.

تهدف حقوق الإنسان الرقمية إجمالاً إلى ضمان الحرية والسلامة والأمان في الخدمات المتوفرة في البيئة الرقمية، إذ أكد منتدى الأمم المتحدة لحوكمة الإنترنت على دور هذه الحقوق في تحقيق الأهداف التنموية وتحسين مستوى الحياة الاجتماعية (IGF, 2019). ونظراً للارتباط الوثيق بين حقوق الإنسان وحرياته الأساسية وتقنيات الاتصال الحديثة، ومع تغلغل تقنيات المعلومات وتكنولوجيات الاتصالات ـ وخصوصاً الإنترنت ـ في حياة المجتمعات البشرية اليومية، أضحت الحقوق الرقمية بمثابة حجر الزاوية corner stone والعمود الفقري backbone لمجتمع المعلومات العالمي، بحيث أصبح لا يمكن إغفال أبعادها الاجتماعية والاقتصادية والسياسية ذات الأهمية الأمنية المتزايدة.

فعلى الصعيد الاجتماعي، تعتمد مجتمعات المعلومات ـ التي يكون فيها لصناعة المعلومة ونشرها والنفاذ إليها واستخدامها أثر كبير في مختلف النواحي ـ بشكل متنامٍ على تكنولوجيا الاتصالات والمعلومات وخدمات الشبكة العالمية، بيد أن هذا الاعتماد المطرد رافقته مجموعة من المخاطر والتهديدات الرقمية، التي من شأنها الإضرار بحقوق الأفراد وتهديد أمنهم وسلامتهم. وهنا تبرز الأبعاد الاجتماعية لحقوق الإنسان الرقمية ـ وفق المفهوم السابق بيانه ـ في حماية البيانات الشخصية للأفراد وتأمينها ضد ممارسات الابتزاز والتلاعب وإساءة الاستغلال، إذ أن من أهم نتائج حماية الحقوق الرقمية منع وقوع مستخدمي الإنترنت ضحايا للإجرام الإلكتروني.

كما يظهر البعد الاجتماعي للحقوق الرقمية في الوقاية من جرائم الأموال التي يتعرض لها أفراد المجتمع عند استخدامهم المتزايد للخدمات الإلكترونية؛ مثل الخدمات المصرفية online banking، وأنظمة الدفع الإلكتروني للفواتير، والتسوق عبر الإنترنت، حيث غالباً ما يقع الأفراد ضحية الغش أو الاحتيال عن طريق

خداعهم بمواقع إلكترونية زائفة أو ببريد إلكتروني وهمي، يستهدف اختراق كلمات المرور أو سرقة بيانات الدفع payment data أو استنساخ البطاقات المصرفية، لأغراض الإتجار أو التهديد بها، وغير ذلك من انتهاكات مرتبطة بالحصول على المال بطرق احتيالية. في المقابل تشكل الحقوق الرقمية درع ضد استغلال البيئة الرقمية للإضرار بأمن المعلومات وأعضاء المجتمع المعلوماتي، لاسيما المعلومات الشخصية وأمن الفئات المستضعفة كالأحداث وذوي الاحتياجات الخاصة. وبذلك يعتبر الأمن الرقمي بمثابة صمام أمان لحماية مجتمع المعلومات، و"بناء الثقة والأمان في استعمال تكنولوجيا المعلومات والاتصالات" (Gercke, 2014).

وعلى الصعيد الاقتصادي، تُسهم الحقوق الرقمية على نحو متزايد في تحقيق التنمية المستدامة ودعم الازدهار الاقتصادي من خلال حماية المصالح المالية للأفراد في التعاملات الإلكترونية وتشجيع استخدام تكنولوجيات المعلومات والاتصالات بما يعود بالنفع على مصالح الأمن القومي. فمع التوجه الحالي للدول العربية نحو الحكومة الإلكترونية والتجارة الإلكترونية والتعليم الإلكتروني والصحة الإلكترونية، والتي تعتبر جميعها بمثابة تطبيقات رقمية حديثة، تبرز الحاجة إلى الحقوق الرقمية لحماية هذه الأنظمة الخدمية وغيرها من البنى التحتية الوطنية للمعلومات، وذلك بما يضمن احترام حقوق الإنسان الرقمية وأمن المستخدمين وسلامتهم المعلوماتية، وصولاً إلى تحقيق الأمن الرقمي والاقتصادي للدولة، لا سيما في ظل الأزمات، كأزمة جائحة كورونا.

ولعل ما يبرز الدور الاقتصادي للحقوق الرقمية هو الارتباط الوثيق بين الإضرار بالمصالح الشخصية للأفراد والإخلال بالمصالح الاقتصادية للدولة؛ بمعنى أن عدم تأمين الحقوق الرقمية أو عدم كفايتها من شأنه أن يؤدي إلى تعطيل مصالح الأفراد وتعريض الاقتصاد الوطني للخطر، مما يدلل على ارتباط منظومة الأمن الرقمي بالمنظومة الاقتصادية في الدولة. وأقر الاجتماع السنوي للمنتدى الاقتصادي العالمي لعام ٢٠٢٠ World Economic Forum (WEF) Annual Meeting الذي عُقد في سويسرا، بارتفاع المخاوف العالمية حول المخاطر التكنولوجية وخصوصاً انتهاكات الحقوق الرقمية التي قد تؤثر على قطاعات اقتصادية حيوية. كما أكدت منظمة التجارة العالمية (WTO) على الأدوار المستقبلية المعقودة على الأمن الرقمي في تأمين التجارة الدولية الرقمية (World Trade Report, 2018).

أخيراً، وعلى الصعيد السياسي، تعتبر الحقوق الرقمية عنصراً جوهرياً لصيانة كيان الدول والحفاظ على أمنها واستقرارها، بحيث أصبح الأمن الرقمي الآن على رأس الأجندة السياسية الإقليمية والدولية، وفي مقدمة أولويات الدول وأجهزة الأمن، خاصة بعد استفحال الاعتداءات الإلكترونية ووقوع الكثير من الأفراد في براثن الجريمة المعلوماتية. وتؤكد المادة (٤) من ميثاق الحقوق الرقمية الأساسية للاتحاد الأوروبي على مسؤولية الدولة في حماية مستخدمي الإنترنت، وذلك باعتبارها الوصي والمسؤول عن الضمانات التي تمنع انتهاكات حقوق الإنسان الرقمية. ويرى البروفسور Helmbrecht (الرئيس التنفيذي للوكالة الأوروبية لأمن الشبكات)

بأن "تعزيز الثقة والأمن في البيئة الرقمية لم يعد خياراً بالنسبة للدول؛ وإنما متطلب أساسي وشرط مسبق للانضمام للمجتمع الدولي للمعلومات، مما يستوجب على الدول القيام بمسؤولياتها في تأمين الاعتماد المتزايد على الاتصال الرقمي البيني" (Christou, 2016).

والحقيقة أنه وبعيداً عن الالتزامات الدولية، يبقى الحفاظ على الحقوق الرقمية وتحقيق الأمن الرقمي مطلب شعبي وهدف قومي يُشكل جزءاً أساسياً من السياسة الأمنية الوطنية، لاسيما وأن الدولة ذاتها قد تتعرض لإشاعات مغرضة أو خطابات عنف وكراهية أو أفكار هدامة تستهدف أمنها واستقرارها ووحدتها، بالإضافة إلى ضرب سلامتها المعلوماتية وشبكاتها الرقمية، مما يؤثر في هيبتها الوطنية ومكانتها السياسية. وقد تنبهت العديد من الدول لهذه الأبعاد السياسية، وباتت تصنف مسائل الأمن الرقمي كأولوية سياسية political priority في استراتيجياتها الأمنية، فعلى سبيل المثال، تنص الاستراتيجية الألمانية للأمن الرقمي digital security strategy for Germany صراحةً على أنه يجب أن تحافظ ألمانيا على سيادتها ومصالح مواطنيها في البيئة الرقمية من خلال بناء قدرات إلكترونية قوية ومستدامة لكل مستوى من مستويات الحكومة.

فكما يرتبط الأمن الرقمي بالاقتصاد الرقمي digital economy؛ بحيث يؤدي شيوع احترام الحقوق الرقمية وتوفير بيئة رقمية آمنة إلى دعم الاقتصاد الوطني نحو التحول إلى اقتصاد رقمي متين، فإن الأبعاد الاجتماعية والاقتصادية والسياسية لحقوق الإنسان الرقمية ترتبط أيضاً بالأمن الرقمي لأفراد المجتمع؛ بحيث يترتب على فهم واستيعاب الكوادر الشرطية لهذه الأبعاد، حماية وتعزيز منظومة الأمن الوطني الشامل. ووفقاً لقرار الجمعية العامة للأمم المتحدة رقم (٥٦/١٢١) بشأن مكافحة الاستخدام الإجرامي لتقنيات المعلومات Combating the Criminal Misuse of Information Technologies، "ينبغي على الدول أن تضمن عدم توفير ملاذات آمنة لأولئك الذين يسيئون استخدام تكنولوجيا المعلومات بشكل إجرامي".

وإنطلاقاً من ذلك، صنف الدليل العالمي للأمن السيبراني الذي تصدره الأمم المتحدة ممثلةً في الاتحاد الدولي للاتصالات Global Cybersecurity Index (GCI) 2020 دول العالم فيما يتعلق بالأمن الرقمي إلى ثلاث مستويات: ١- دول عالية الإلتزام (كالسعودية والإمارات وعُمان ومصر وقطر)؛ ٢- دول متوسطة الإلتزام (كالمغرب وتونس والأردن والبحرين والكويت والجزائر والسودان)؛ ٣- دول ضعيفة الإلتزام (كلبنان وليبيا وفلسطين وسوريا والعراق وموريتانيا والصومال وجزر القمر وجيبوتي واليمن). وعلى الرغم من أن هذا التصنيف الدولي لإلتزام الدول بمعايير الأمن الرقمي ليس له تبعات قانونية مؤكدة، إلا أنه ــ بلا شك ــ له تبعات اجتماعية واقتصادية وسياسية ذات تأثير على مراكز الدول ومكانتها وأمنها وفرصها التنموية المستقبلية.

بعد مناقشة الأبعاد الثلاثة الرئيسية لحقوق الإنسان الرقمية، يُلاحظ الارتباط الوثيق بين هذه الحقوق وكافة حقوق الإنسان الأخرى الاقتصادية والاجتماعية والثقافية والسياسية؛ بمعنى أن احترام حقوق الإنسان الرقمية له

أبعاده وآثاره الإيجابية، أما انتهاكها فله عواقبه وآثاره الوخيمة، ليس فقط على ممارسة هذه الحقوق الأساسية، وإنما على المنظومة الشاملة للأمن الوطني، وبخاصة إذا نُسب الانتهاك للأجهزة الأمنية. وعليه، كان لزاماً على الكوادر الأمنية العربية الوعي التام بهذه الحقوق الحديثة والإلمام الكامل بها، نظراً لأهمية ذلك في تعزيز حقوق الإنسان وحمايتها في مجتمع المعلومات، ومن بينها المجتمعات العربية.

المطلب الثالث
أهميـة إلمام الكوادر الشرطية العربية بحقوق الإنسان الرقمية

إن وظيفة الشرطة وإن كانت صعبة وشاقة، فهي في الواقع وظيفة مشرفة وحيوية لأمن وسلامة المجتمع واستقراره، ويكفي رجال الشرطة فخراً اعتراف الإعلان العالمي لحقوق الإنسان بهذه الحقيقة ضمناً منذ أكثر من نصف قرن، كما نصت على ذلك صراحةً العديد من صكوك الأمم المتحدة لحقوق الإنسان، بما فيها "مدونة قواعد سلوك الموظفين المكلفين بإنفاذ القوانين" لعام ١٩٧٩، و"المبادئ الأساسية بشأن استخدام القوة والأسلحة النارية من جانب الموظفين المكلفين بإنفاذ القوانين" لعام ١٩٩٠، وطائفة أخرى من الإعلانات والمبادئ التوجيهية الأممية، والتشريعات الوطنية.

وباعتبار منتسبي الشرطة هم خط الدفاع الأول في صيانة حقوق الإنسان، يجب عليهم أولاً معرفة هذه الحقوق والإلمام بها من أجل احترامها وحمايتها، وهو ما تطرق إليه بالتفصيل المطلب الأول من هذا المبحث. ويؤكد الباحث على أنه من غير الصواب افتراض أن حقوق الإنسان الرقمية ـ باعتبارها تتألف من مجموعة من حقوق الإنسان في مجتمع المعلومات ـ ليست ذات أولوية أو لا تتصل بعمل الشرطة اليومي، فمن الأمثلة الجلية للحقوق الرقمية ذات الصلة المباشرة بالعمل الشرطي، الحق في عدم التعرض للابتزاز الإلكتروني، والحماية من ممارسات انتهاك الخصوصية، وسرقة البيانات الشخصية أو إتلافها، والوقاية من الإرهاب الرقمي digital terrorism، واحترام المعايير الأساسية للتمتع بالسلامة والكرامة في الفضاء الرقمي.

وبناءً عليه، تختص الشرطة بحماية طائفة عريضة من حقوق الإنسان الرقمية، مما يحتم الوعي بها وإدراك المسؤولية الوظيفية والأمنية تجاهها، حيث تنص معظم الدساتير العربية على واجب الشرطة وهيئات الأمن العام في كفالة الطمأنينة والأمن وحفظ النظام والآداب العامة وفقاً للقانون. فإذا كانت الدولة وفقاً للدستور هي المسؤولة عن توفير الأمن والطمأنينة لمواطنيها ولكل مقيم على أراضيها، فإن الشرطة هي الذراع الأمين للدولة في تنفيذ هذه المهام الجسام والمسؤوليات العظام، وهي من يلتزم واقعاً باحترام وحماية حقوق الإنسان على الوجه المبين في القانون.

وترجمةً لهذه المبادئ الدستورية، تنص قوانين الشرطة العربية على اختصاص الشرطة بالمحافظة على النظام العام والأمن العام والآداب، وحماية الأرواح والأعراض والأموال، وكفالة الطمأنينة والسكينة في كافة

المجالات. ولا شك أن المجال الرقمي من أكثر المجالات ـ إن لم يكن أكثرها ـ إتصالاً بحياة الناس، حيث يتميز أسلوب الحياة المعاصرة في كل أنحاء العالم بالاعتماد الأساسي على الإنترنت وتقنية المعلومات في كافة نواحي الحياة الاجتماعية والتعليمية والصحية والاقتصادية والصناعية والأمنية، وقد أظهرت دراسة حديثة أن عدد مستخدمي الإنترنت في مصر مثلاً يبلغ ٥٩,١٩ مليون بنسبة ٥٧,٣٪ من عدد السكان، بينما يصل عدد المستخدمين في السعودية إلى ٣٣,٥٨ مليون بنسبة ٩٥,٧٪ من عدد السكان (Digital Reports, 2021).

أمام هذا الواقع الرقمي المعاش، ينبغي على رجال الشرطة إيلاء عناية خاصة بحقوق الإنسان الرقمية والعمل على منع انتهاكها وضبط ما يقع من اعتداءات عليها، وهو ما لا يتأتى إلا بفهم طبيعة هذه الحقوق وتنفيذ ما تفرضه القوانين واللوائح ذات العلاقة. ومن النماذج التشريعية الرائدة في مجال احترام حقوق الإنسان في العمل الشرطي، ما يفرضه صراحةً قانون سلوك الشرطة الإنجليزي لسنة ٢٠١٢م (The Police (Conduct Regulations من واجبات على منتسبي الشرطة "بعدم تجاوز سلطاتهم أو صلاحياتهم واحترام حقوق جميع الأفراد". ويعتبر (دليل معايير وممارسات حقوق الإنسان في عمل الشرطة) Human Rights Standards & Practice for the Police الصادر عن مكتب الأمم المتحدة لحقوق الإنسان عام ٢٠٠٤، المصدر التاريخي للنص الإنجليزي؛ حيث أرسى قاعدة عامة بأنه "يجب على مسؤولي إنفاذ القانون احترام وحماية كرامة الإنسان والحفاظ على الحقوق الأساسية لجميع الأفراد".

فهذه المعايير الدولية والنصوص القانونية ذات الصلة بعمل الشرطة وحماية حقوق الإنسان تم وضعها لا لعرقلة إنفاذ القوانين، وإنما لتوفير ضوابط ومعايير أخلاقية من شأنها الارتقاء بالأداء الشرطي وفعالية الوظيفة الشرطية في المجتمع الرقمي دون مساس بحقوق الإنسان، ومن ثم تنسف صحة المقولة القديمة بأنه من أجل تطبيق القانون وضمان إدانة المجرمين "لابد من الخروج على القانون قليلاً". فهذا الادعاء الزائف الذي يبرر انتهاك حقوق الإنسان في سبيل تحقيق الإنفاذ الفعال للقوانين، لا يسعه إلا أن يزيد الأمور سوءاً وتدهوراً ويزج بمنتسبي الأجهزة الأمنية المخالفين في مهاوي المساءلات الجنائية والتأديبية، وفق ما تقضي به التشريعات، ناهيك عن الإضرار بحقوق الضحايا، وبسمعة ومكانة الشرطة، والدولة بشكل عام.

وفي المقابل، عندما تعي الشرطة والأجهزة الأمنية حقوق الإنسان الرقمية وتوطدها وتضمن احترامها، فإن ذلك يعزز بالفعل من فاعليتها ويعزز الثقة العامة وتعاون الجمهور ويؤدي إلى حصولها على الدعم المجتمعي، ومن ثم تصبح الشرطة قادرة على منع الجريمة ومكافحتها من خلال الأخذ بزمام المبادرة وتطبيق القانون على بصيرة وعن يقين، مما يساهم في نجاح المحاكمات الجنائية وإقامة العدل والنظام في الدولة. ويرى الباحث أن من أهم مظاهر تطبيق مفهوم "دولة القانون والمؤسسات" هو إلمام الكوادر الأمنية بالمبادئ القانونية لحقوق الإنسان الأساسية والرقمية بإعتبارها ركيزة من ركائز المجتمعات المتحضرة في عصرنا الرقمي الحالي.

وإدراكاً من مفوضية الأمم المتحدة لحقوق الإنسان OHCHR لأهمية الجانب التوعوي في العمل الشرطي، قامت بإعداد سلسلة تدريبية ثرية مصممة خصيصاً لتوعية منتسبي الشرطة بمعايير وممارسات حقوق الإنسان، بمسمى "المرشد في حقوق الإنسان لمدربي الشرطة" Police And Human Rights Manual for Police Training، والتي يمكن تبنيها وتطويرها لتنسجم أكثر مع طبيعة وتقاليد المجتمعات العربية. كما قام معهد تدريب الشرطة بوزارة الداخلية القطرية بإعداد كتاب إرشادي بعنوان "مبادئ حقوق الإنسان في العمل الشرطي". وتنفذ الكثير من أجهزة الشرطة العربية دورات تدريبية متخصصة في مجال حقوق الإنسان.

وبالرغم من هذه الجهود التوعوية والبرامج التدريبية، كشف الاستبيان المستخدم في هذه الدراسة بأن قرابة ٨١٪ من رجال الشرطة العرب المجيبون على الاستبيان لم يتلقوا تدريباً للتوعية بحقوق الإنسان الرقمية، مما يدق ناقوس الانتباه ويبرز الحاجة الملحة إلى مواصلة العمل وتكثيف الجهود في هذا المجال، الذي وصفه أحد المجيبين على الاستبيان بأنه "اضعف حلقة" في العمل الشرطي، كما أقترح أحد المجيبين ضرورة تصميم موقع إلكتروني شرطي ـ أسوة بموقع شرطة الإنتربول التدريبي INTERPOL Virtual Academy ـ يقدم معلومات توعوية وبرامج تدريبية للكوادر الشرطية في مجالات حقوق الإنسان الرقمية. ولا شك أن الاستثمار في هذا الجانب هو استثمار ذو عائد مضمون؛ فعندما تصبح الكوادر الشرطية ملمةً بحقوق الإنسان الرقمية في مختلف التعاملات والمواقف، فإن مردود ذلك كبير ومباشر على استقرار وازدهار المجتمع، من خلال احترام حقوق المستخدمين الرقمية وسلامتهم المعلوماتية، وصولاً إلى تحقيق الأمن الرقمي للدولة.

مما سبق ذكره في هذا المبحث، يتضح بأن حقوق الإنسان الرقمية تُمثل تجسيداً لحقوق الإنسان الأصيلة، ولكن في البيئة الرقمية ذات الطبيعة المتجددة، بالإضافة إلى طائفة مستحدثة من الحقوق الأساسية لا غنى للأفراد عنها في مجتمع المعلومات. وبالنظر إلى أبعادها الاجتماعية والاقتصادية والسياسية، تكتسب الحقوق الرقمية أهمية أمنية خاصة، تستوجب ليس فقط إلمام الكوادر الشرطية العربية بها، وإنما العمل بجهد ووعي وحكمة لتأمينها وترسيخ احترامها، وذلك لكونها تُشكل في جوهرها ضمانات قانونية عالمية لحماية الأفراد والجماعات من الانتهاكات الرقمية والاعتداءات الإلكترونية التي تمس بالحريات الأساسية والكرامة الإنسانية.

فالتشريعات الرقمية التي ينبغي الإلمام بها ـ وفق ما سوف يبين المبحث الثالث ـ تنقسم إلى مجموعتين أساسيين هما: تشريعات مدنية وإدارية تتعلق بتنظيم الخدمات الرقمية وأمن الاتصالات الرقمية digital security legislations وتشريعات جنائية خاصة بمكافحة الجرائم الرقمية digital criminal legislations. وتتميز التشريعات الجنائية بصفتها العقابية الرادعة وباشتمالها على تدابير صارمة، لذلك يُعول على تطبيقها بشكل مهني واحترافي كثيراً في توفير بيئة مجتمعية آمنة من شأنها التصدي لتطورات ومخاطر الانتهاكات الرقمية.

المبحث الثاني
الانتهاكات والمخالفات الماسة بحقوق الإنسان الرقمية

تمهيد وتقسيم:

أضحت حقوق الإنسان الرقمية بمثابة ضمانة قانونية هامة ومظلة أمنية فاعلة يستظل بها الأفراد والمؤسسات في الفضاء الرقمي المفتوح، وفي المقابل تشير التقارير الدولية إلى تصاعد وتيرة المخاطر والانتهاكات الرقمية. وقد أكد قرار الجمعية العامة للأمم المتحدة رقم (٧٠/١٢٥) لسنة ٢٠١٥م بشأن تنفيذ نتائج القمة العالمية لمجتمع المعلومات على أنه في حين أظهرت تكنولوجيا الاتصالات والمعلومات قدرة فائقة على تعزيز ممارسة حقوق الإنسان وتمكين الوصول إلى المعلومات وحرية التعبير والتجمع السلمي وتكوين الجمعيات، إلا أن هناك قلق عميق إزاء الانتهاكات والتهديدات الخطيرة التي تتعرض لها حقوق الإنسان الرقمية، الأمر الذي يستدعي تدخل الدول وأجهزتها الأمنية لاتخاذ كافة التدابير اللازمة لضمان حماية مختلف الحقوق الرقمية (UN, A/RES/70/125, p.9).

كما أشارت المنظمة الدولية للشرطة الجنائية INTERPOL في تقرير لها أن جائحة كورونا coronavirus pandemic الحالية أحدثت سلوكيات رقمية جديدة تمثلت في لجوء مليارات الأشخاص إلى الإنترنت للتسوق والعمل والدراسة وإنجاز العديد من المعاملات التي عطلها الإغلاق الكلي أو الجزئي، مما وسع من نطاق الاعتداءات الرقمية لتشمل عمليات التضليل والاحتيال والتصيد الإلكتروني ونشر البرمجيات الخبيثة وبرامج التجسس وسرقة البيانات (INTERPOL's COVID-19 global threat assessment, 2020). وفي تقرير حديث صادر عن منظمة العفو الدولية AMNESTY International، تشير البيانات عن رصد ممارسات غير قانونية واسعة لأنشطة مراقبة إلكترونية تعسفية وانتهاك للخصوصية الرقمية (AMNESTY, Digital Surveillance, 2020).

وتختلف الدراسات في تقسيم الانتهاكات أو الاعتداءات أو الجرائم الرقمية، وذلك بالنظر إلى أهدافها ودوافعها وضحاياها ونطاقها والآثار المترتبة عليها، إلا أن هذه الدراسة سوف تعتمد تقسيماً لانتهاكات حقوق الإنسان الرقمية يقوم على أساس النظر إلى طبيعة آثارها ونوعية الحق الرقمي المعتدى عليه. بناءً عليه، يستعرض هذا المبحث من خلال المطالب الثلاثة الآتية، ثلاثة طوائف رئيسية، تمثل أخطر انتهاكات حقوق الإنسان الرقمية، وتتطلب يقظة وانتباه الكوادر الشرطية العربية.

المطلب الأول
الانتهاكات المتعلقة بالجانب المالي لحقوق الإنسان الرقمية

لابد من الإشارة في البداية إلى أن مصطلح الاعتداءات أو الانتهاكات الرقمية ذو مدلولات واسعة يشمل كافة الأعمال والممارسات الضارة التي لا تخضع لنصوص قانونية صريحة، ولكن بسبب خطورتها تكون محل اهتمام الأجهزة الأمنية، بينما يقتصر مصطلح "الجرائم الرقمية" على الأفعال المعاقب عليها بموجب نصوص قانونية تصفها وتحدد عناصرها بدقة، تطبيقاً لمبدأ شرعية الجرائم والعقوبات القائل بأنه "لا جريمة ولا عقوبة إلا بناء على قانون". فبسبب التطور السريع والمتلاحق في مجالات التكنولوجيا الرقمية وتقنية المعلومات وأجهزة الاتصالات لم تتمكن معظم التشريعات من مواكبة هذه التطورات الرقمية بشكل متواصل ومتلازم.

وتشير التقارير الصادرة عن المنظمة الدولية للشرطة الجنائية إلى استخدام عدة مصطلحات في هذا الشأن؛ كـ "جرائم الإنترنت" Internet Crimes، و"جرائم المعلومات" Information Crimes، و"الجرائم الرقمية" Digital Crimes، و"الجرائم الإلكترونية" Cyber Crimes، إلا أن هذه المصطلحات ـ وخصوصاً جرائم المعلومات التي تهتم أساساً بسرية البيانات ـ أضيق نطاقاً من الاعتداءات الرقمية التي تتسع لكل الانتهاكات التي تقع في الفضاء الرقمي ولم تطلها النصوص التشريعية. وفي هذا الصدد أشارت منظمة الإنتربول في تقرير حديث لها بأن الاعتداءات الرقمية ـ كالاحتيال والاختراق والقرصنة الرقمية ـ تمثل تهديدات جرمية حقيقية للغاية تواجه أجهزة الشرطة في جميع أنحاء العالم على أساس منتظم وبشكل متزايد (INTERPOL, Digital Security Challenge, 2020).

فمع زيادة الاعتماد على الإنترنت وزيادة عدد المتصلين بالفضاء الرقمي، تزداد احتمالات الاعتداءات الرقمية. وقد بينت دراسة حديثة أن نسبة نمو مستخدمي الإنترنت حول العالم قد بلغت ١٥,٥ مستخدم جديد كل ثانية، بمعدل ١,٣ مليون مستخدم جديد كل يوم، ليبلغ عدد مستخدمي الإنترنت حول العالم في يناير ٢٠٢١م ٤,٦٦ مليار شخص، أي ما نسبته ٥٩,٩٪ من سكان العالم البالغ ٧,٨٣ مليار نسمة (DIGITAL 2021: Global Overview Report). وفي الدول العربية، بلغ عدد مستخدمي الإنترنت في عام ٢٠١٩ حوالي ٢٥٠ مليون مستخدم، بنسبة ٥٤,٦٪ من عدد السكان، ويستخدم أكثر من ٢٠٠ مليون شخص عربي الهواتف الذكية smart phones الموصولة بالإنترنت (Digital trends in the Arab States region ITU, 2021)، حيث تجاوزت النسبة في دولة قطر ـ على سبيل المثال ـ عدد السكان لتبلغ ١٦٠,٦٪ (DIGITAL 2021)، مما يعني أن الأجهزة الرقمية أصبحت عنصراً أساسياً لا غنى عنه في ممارسة شؤون الحياة اليومية.

وتتمثل أبرز الاعتداءات والجرائم التي تمس الحقوق المالية للمستخدمين في عمليات النصب والاحتيال والغش الإلكتروني phishing، وسرقة الأموال والعملات الرقمية blockchain، وتزوير الشيكات الرقمية digital checks، وتزييف بطاقات الائتمان credit cards، وانتهاك حقوق الملكية الفكرية والصناعية IPRs، والاعتداء على العلامات التجارية، وإفشاء الأسرار التجارية، والغسل الإلكتروني للأموال، واختراق أنظمة المعلومات المرتبط بطلب فدية، وقرصنة الحسابات والبيانات المصرفية، وغيرها من الأفعال التي تستهدف النيل من الحقوق المالية للمستخدمين.

ومما ضاعف من أخطار هذه الجرائم وصعب من ملاحقتها استخدامها لأساليب جرمية بالغة التعقيد كالهجمات المؤتمتة automated attacks، والاعتداءات البوتنتية Botnets، وتقنيات التشفيرencryption techniques، والحوسبة السحابية cloud computing، وتقنيات الذكاء الاصطناعي artificial intelligence التي تتيح للآلات والبرامج محاكاة القدرات الذهنية البشرية، والاتصالات عبر بروتوكول الإنترنت VoIP التي ترفع من عدد الهجمات ولا تتيح تعقبها أو كشف مستخدميها، بالإضافة إلى الإنترنت المظلم darknet وما يتيحه من سلع غير مشروعة وخدمات المرتزقة.

غني عن البيان، أن الهجمات الرقمية الخبيثة تُمثل خطراً متنامياً يواجه ليس الأفراد فقط، وإنما تهديداً جدياً من شأنه زعزعة الاستقرار المالي والاقتصادي للدول والأنظمة التجارية العالمية. ومن الأمثلة البارزة على الضرر الاقتصادي البليغ الذي تلحقه البرمجيات الخبيثة، عملية الاحتيال الكبيرة التي تعرض لها عملاء شركة "آبل" Apple العملاقة مؤخراً حيث تم استهداف مستخدمي حواسيب ماك وسرقة قرابة ٤٠٠ مليون دولار من حساباتهم. وعلى صعيد المصارف الحكومية، تعرض البنك المركزي لدولة بنغلاديش في عام ٢٠١٦ لقرصنة أدت إلى سرقة ٨١ مليون دولار من حسابه في بنك نيويورك الفيدرالي، لذلك لا غرابة في أن يصنف صندوق النقد الدولي IMF الاعتداءات الرقمية كأعظم المخاطر التي تهدد الاستقرار المالي العالمي في عام ٢٠١٨ والسنوات القادمة (IMF, Cyber Risk for the Financial Sector, 2018). وتتوقع مراكز بحثية بأن الحقوق المالية الرقمية ستكون أكثر عرضة للخطر مع ازدهار عمليات الدفع الإلكتروني banking systems عبر الهاتف المحمول (Cybersecurity Trends, 2020).

ويظهر المساس المباشر لهذه الانتهاكات والجرائم الإلكترونية بحقوق الإنسان الرقمية من خلال أولاً انتهاك حق الأفراد في النفاذ إلى فضاء رقمي آمن وموثوق، وثانياً التعدي على حق الأفراد في التمتع بالسلامة المالية والائتمانية، وثالثاً الإضرار بالذمة المالية للأفراد وحرمة أموالهم وممتلكاتهم الخاصة، ورابعاً الإساءة إلى القطاعات الخدمية المالية والخدمات المصرفية، وخامساً تقويض النظام المالي العالمي والإخلال بالاقتصاد الوطني الذي يمثل الحاضنة الآمنة والدعامة الأساسية لحقوق الإنسان الاقتصادية وموارد التنمية الاجتماعية.

المطلب الثاني
الانتهاكات المتعلقة بالجانب الأخلاقي لحقوق الإنسان الرقمية

لا تقتصر الانتهاكات في الفضاء الرقمي على المصالح المالية، وإنما تلحق الاعتداءات أيضاً القيم الأخلاقية المتعارف عليها في النظم الاجتماعية والاقتصادية. وبالرغم من أنه وبخلاف الطائفة الأولى من الانتهاكات الرقمية ذات الطابع المالي أو المادي، تتسلط الجرائم الأخلاقية عبر الإنترنت أساساً على القيم الإنسانية الاجتماعية أو المظهر المعنوي للشعوب، إلا أن هذا المظهر اللامادي أو الطابع المرئي والمقروء للانتهاكات الرقمية الأخلاقية لا يقلل من جسامتها وخطورتها على الأخلاقيات الذاتية للشعوب العربية. وإدراكاً لذلك، نصت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة ٢٠١٠م على أنها تهدف إلى حماية المجتمع العربي ضد جرائم تقنية المعلومات التي تهدد أمن ومصالح وسلامة المجتمعات العربية، وكذلك المبادئ الدينية والأخلاقية السامية والتراث الإنساني للأمة العربية.

فبينما مكنت وسائل التواصل الاجتماعي social media على الإنترنت ـ بما في ذلك واتساب WhatsApp وانستجرام Instagram وتويتر Twitter وفيسبوك Facebook وتيك توك TikTok وسناب شات Snapchat ـ كافة أفراد المجتمع بمختلف أجناسهم وأعمارهم من إنشاء أي محتوى سريعاً ومشاركته مع الجمهور، بالإضافة إلى تبادل الصور ومقاطع الفيديو والوثائق والتسجيلات الصوتية، فإن مستخدمي هذه التطبيقات غالباً ما يتعرضون لاعتداءات أخلاقية تمس بحقوقهم الرقمية وكرامتهم الإنسانية.

إذ كشف تقرير (DIGITAL 2021) عن الشعبية الكبيرة التي تحظى بها وسائل التواصل الاجتماعي في أوساط المجتمعات العربية، حيث بلغ عدد مستخدمي هذه الوسائط الرقمية في مصر مثلاً ٤٩ مليون شخص، أي ٤٧,٤٪ من عدد السكان، وفي المغرب ٥٩,٣٪، والأردن ٦١,٥٪، ولبنان ٦٤,٣٪، وتونس ٦٩٪، والسعودية ٧٩,٣٪، وعُمان ٨٠,٢٪، والكويت ٩٨,٨٪. في المقابل، ورد في تقرير شركة Kaspersky الدولية المتخصصة في الأمن الرقمي أن الدول العربية جميعها تعرضت لأكثر من ١٥٠ مليون هجمة إلكترونية malware attacks على مستخدمي الهواتف الذكية من يناير حتى يونيو ٢٠٢٠م، وتقدر نسبة مستخدمي الهواتف الذين تعرضوا لهجمات خبيثة بـ ٢١,٩٪ في لبنان، و٢٩,٢٪ في مصر، و٣١,٣٪ في عُمان، و٣٤,٢٪ في قطر، و٣٥،٩٪ في السعودية (Kaspersky, Digital Dangerscape, 2020).

وتُعد هذه المعدلات مرتفعة مقارنةً بالمستويات الدولية والإقليمية، ويمكن تصنيف الانتهاكات الماسة بالجانب الأخلاقي لحقوق الإنسان الرقمية إلى ثلاث فئات رئيسية: تتضمن الفئة الأولى أفعال سرقة البيانات الشخصية للأفراد ونشرها على الإنترنت دون أذن، وسرقة الصور والملفات الخاصة وتسريبها أو استخدامها دون وجه حق digital piracy، والابتزاز والتهديد الإلكتروني، والقذف والسب والتشهير، وأعمال السحر والشعوذة

على الإنترنت. ويندرج تحت الفئة الثانية ممارسات استدراج الأطفال والمراهقين بغية استغلالهم جنسياً child pornography، ونشر المواد الإباحية والمحتوى غير المشروع، والتحرش الجنسي وملاحقة النساء، وممارسة الدعارة والقمار، وترويج المخدرات والمؤثرات العقلية عبر الإنترنت. أما الفئة الثالثة فتشمل أفعال بث الكراهية والعنف، والتحريض ضد الأقليات، والدعوة للتمييز العنصري، ونشر الأفكار الإرهابية والمتطرفة، والترويج للإشاعات المغرضة، وإهانة رؤساء الدول والبعثات الدبلوماسية، والإساءة إلى الأديان، وغيرها من الأفعال التي تتعارض مع الآداب العامة والقيم الدينية والمبادئ الأخلاقية للمجتمعات العربية.

وتجدر الإشارة إلى أن منظمة هيومن رايتس ووتش أصدرت تقريراً في عام ٢٠٢١ ينتقد تقييد حقوق المثليين والمثليات ومزدوجي الميل الجنسي في الدول العربية (Human Rights Watch, World Report, 2021)، ويمكن القول بأن ما تعتبره المنظمة ـ من منظورها الثقافي ـ حقوقاً وحريات جنسية للمثليين، لا تقره الدول العربية التي تحكمها في هذا الشأن مبادئ دينية وأخلاقية، وأعراف وتقاليد اجتماعية تحرَم هذه الممارسات الشاذة ولا تعتبرها حقوقاً، وبالتالي لا يُعد تجريم نشاطات هؤلاء على الإنترنت مساساً بالحقوق الرقمية، لأن هذه الممارسات الجنسية ليست ضمن الحقوق الرقمية التي تقرها وتقبلها المجتمعات العربية.

ولا جدال حول خطورة هذه الممارسات اللاأخلاقية ومساسها المباشر بحقوق الإنسان الرقمية؛ فبالإضافة إلى تهديدها الصريح للنسيج الأسري والمجتمعي والوطني، تسيئ هذه الجرائم بشكل أساسي إلى كرامة الإنسان وسلامته الشخصية عند ممارسته لحقه في النفاذ إلى بيئة رقمية آمنة. إلا أنه من وجهة نظر الباحث فإن مساس الأفعال المتقدمة بحقوق الإنسان الرقمية يظهر بشكل أكثر وضوحاً من خلال تعديها السافر على حق المستخدمين في الخصوصية وسرية بياناتهم الخاصة، وحقهم في التمتع بالحماية اللازمة للشرف والسمعة على الإنترنت، وكذلك حقهم في عدم التعرض للاستغلال والعنف والاعتداء على الشبكة، وحقهم في تصفح المحتوى السليم المتوافق مع المعايير الأخلاقية.

ولا يعني شيوع الانتهاكات الماسة بالجانب الأخلاقي لحقوق الإنسان الرقمية في المجتمع العربي سلامة المجتمعات الأخرى من هذه الاعتداءات، حيث تشهد المجتمعات الأوروبية والأمريكية انتهاكات مماثلة وربما أكثر ضراوةً؛ فمن الأمثلة على الانتهاكات الرقمية المؤثرة تسريبات WikiLeaks في عام ٢٠١٠ لوثائق شخصية ورسمية في غاية السرية، والاختراق الذي تعرض له البريد الإلكتروني الخاص لوزيرة الخارجية الأمريكية هيلاري كلينتون في عام ٢٠١٦، وقرصنة مزود خدمات الويب والبريد الإلكتروني Yahoo في عام ٢٠١٤، وكذلك اختراق بيانات شركة ميكروسوفت العالمية Microsoft Corporation في عام ٢٠١٧، وصولاً إلى الاختراق الشهير لملايين حسابات مستخدمي تويتر Twitter في عام ٢٠٢٠، والذي يجسد على الواقع صحة مقولة بأن العصر الحالي هو عصر الاختراقات الرقمية الكبرى era of major

.(Andress & Winterfeld, 2016, p.30) breaches

ولكن المجتمع العربي ـ بسبب التأخر التقني في مجال الأمن الرقمي ـ في حاجة أكبر إلى بناء قدراته الرقمية وتعزيز الثقة والأمن في إستخدام تكنولوجيا المعلومات والاتصالات، من خلال تطوير إجراءات مكافحة الاختراق والوقاية من الجرائم الرقمية التي تُرتكب عبر الإنترنت وتطال أجهزة الحواسيب الشخصية ونظم المعلومات الوطنية، بهدف الدخول غير المشروع وسرقة البيانات أو الإضرار بها. فكما صرح المدعي العام الأمريكي في بداية الألفية فإن "الحرب ضد التهديدات الرقمية على الإنترنت ستكون أحد أكبر تحديات إنفاذ القانون في القرن المقبل".

المطلب الثالث
مخالفات حقوق الإنسان الرقمية التي تُتهم الأجهزة الأمنية بارتكابها

في مسار آخر مختلف عن انتهاكات حقوق الإنسان الرقمية ذات الطابع المالي والأخلاقي، تتعرض الحقوق الرقمية أيضاً للاعتداء، ولكن هذه المرة ليس من قبل مجرمو الإنترنت أو جهة إجرامية، وإنما بفعل مخالفات تنسب لبعض منتسبي الأجهزة الأمنية بحجة إنفاذ القانون والحفاظ على النظام العام. فبخلاف الانتهاكات العمدية السابق مناقشتها، قد تصدر هذه الانتهاكات أو المخالفات ـ التي سوف يأتي بيانها حالاً ـ غالباً عن أعمال غير عمدية وبغير قصد نتيجة قلة وعي واحتراز أو إهمال أو عدم مراعاة الأنظمة والتشريعات، إلا أنه نظراً لخطورتها وعدم مشروعيتها وتأثيرها السلبي على سمعة البلاد ومصداقية الأجهزة الأمنية ينبغي على الكوادر الشرطية إدراكها والحذر من الوقوع في مغبتها مهما كانت المبررات.

حيث شدد قرار الجمعية العامة للأمم المتحدة رقم (٧٣/١٧٩) لسنة ٢٠١٨م بشأن "الحق في الخصوصية في العصر الرقمي" على أن الشواغل المتصلة بالأمن العام وقمع الإرهاب لا تبرر مراقبة الاتصالات الرقمية أو اعتراضها أو جمع البيانات الشخصية على نحو غير قانوني أو تعسفي، لا سيما عندما تجرى على نطاق واسع (UNGA, A/RES/73/179, p.3). وأعربت مفوضية الأمم المتحدة لحقوق الإنسان في تقرير لها صادر في عام ٢٠١٨ حول "مهددات حقوق الإنسان في الفضاء الرقمي" عن بالغ قلقها إزاء سرعة وتيرة تطور تكنولوجيات المعلومات والاتصالات التي عززت قدرة الحكومات والأجهزة الأمنية على مراقبة الاتصالات واعتراضها وجمع البيانات وتحليلها، مما قد يؤدي إلى انتهاك حقوق الإنسان الرقمية والنيل منها .(A/HRC/34/60, p.7)

وعلى الصعيد العربي، أكد المؤتمر الدولي الأول بشأن "تحديات الأمن وحقوق الإنسان في المنطقة العربية" المنعقد في قطر عام ٢٠١٤ على ضرورة الوعي بأن انتهاك حقوق الإنسان بدعوى الحفاظ على الأمن لم يعد

خياراً مقبولاً لدى الشعوب العربية، حيث تثبت الوقائع دوماً بأن التجاوزات الحقوقية من شأنها الإخلال بالأمن وتهديد الاستقرار. كما أوصى المؤتمر الدولي الثاني المنعقد في تونس عام ٢٠١٥ حول ذات الموضوع بأهمية وضع آليات للرقابة والمساءلة لمنع أي محاولات استغلال لصلاحيات وسلطات جهات الأمن وإنفاذ القانون في أعمال تدخلية أو إجراءات تعسفية ضد حقوق الإنسان، لا سيما حقوق الأفراد في الخصوصية الرقمية، بحيث ينبغي مواءمة التشريعات العربية المتعلقة بالأمن وحقوق الإنسان مع المعايير والمواثيق الدولية.

وبمراجعة التقارير الدولية الموثوقة والمستندة إلى الأوضاع الراهنة، يمكن وصف انتهاكات وتجاوزات حقوق الإنسان الرقمية التي تُتهم الأجهزة الأمنية بارتكابها بأنها تجاوزت الوسائل التقليدية غير المشروعة المتمثلة في التنصت على المكالمات وتسجيل الاتصالات وفض الرسائل وقراءتها بدون إذن قضائي، ووصلت إلى توظيف نظم تكنولوجية وأساليب تقنية متطورة لا يسع المجال لذكرها جميعاً، إلا أنه ربما أكثرها اتصالاً بالعالم العربي، استخدام عمليات المراقبة الرقمية السرية واعتراض الاتصالات الإلكترونية على نطاق واسع mass digital surveillance والتي تسمح بمراقبة كافة رسائل البريد الإلكتروني ومكالمات الفيديو والرسائل النصية والمواقع الشبكية التي تمت زيارتها. كما تم رصد استخدام تقنيات الاختراق الحاسوبي الهجومية offensive hacking techniques التي تتيح التسلل إلى الأجهزة الرقمية للأفراد والاطلاع عن بُعد وبشكل سري على محتوى الأجهزة الشخصية والبيانات المخزنة فيها، مما يمكّن من تنفيذ تتبع فوري وإجراء رصد آني للبيانات المتوفرة على هذه الأجهزة ونقلها أو التلاعب بها، سواء كانت مشفّرة أو غير مشفّرة (HRC, Annual report: the right to privacy in the digital age, 2018, p.5-7).

ولعل التقنية الأكثر تطوراً وخطورةً هي تقنية جمع وتحليل البيانات الوصفية metadata aggregation & analysis التي كشف عنها "تقرير مفوض الأمم المتحدة السامي لحقوق الإنسان" بأنها تعمل على جمع كم هائل من بيانات الأفراد عن طريق الحواسيب الشخصية والهواتف والساعات الذكية وأدوات تتبع اللياقة البدنية والملابس التكنولوجية وغيرها من أجهزة الاستشعار الأخرى المترابطة والمثبتة في المنازل والمدن الذكية، ومن ثم تحليل البيانات المتدفقة للتعرف على هوية المستخدم وعناوين بريده الإلكتروني وأرقام هواتفه وبياناته البيومترية والمالية والصحية وأنماط سلوكه وعلاقاته الاجتماعية والأشياء المفضلة لديه وهواياته، كل ذلك وأكثر دون علم الأشخاص المراقبين ودون موافقتهم الفعلية (A/HRC/39/29, 2018, p.4).

وترى منظمة العفو الدولية بأن المراقبة الحكومية بواسطة التكنولوجيات الرقمية البيومترية biometric digital surveillance technologies وكاميرات المراقبة الرقمية خصوصاً في مقاهي الإنترنت تتيح التعرف على ملامح الوجه وتحديد هوية الأشخاص تلقائياً، إلا أن الخطورة تتعاظم عندما يتم ربط هذه التقنيات بتقنيات أخرى لها قدرات تحليلية فائقة كتقنية البيانات الضخمة big data والذكاء الاصطناعي artificial

intelligence التي تستطيع الوصول إلى معلومات بالغة الدقة عن حياة الناس، وإجراء استنتاجات حول خصائصهم البدنية والعقلية، وإنتاج معلومات مفصّلة عن ملامح شخصياتهم المتربطة. وتشير المنظمة إلى وجود أدلة متزايدة على أن المعلومات التي تجمعها المراقبة الحكومية government surveillance عن طريق التجسس واعتراض الاتصالات الرقمية، تتعرض بدورها بشكل متزايد لخطر الاختراق من جانب حكومات معادية أو جماعات إجرامية منظمة، مما يضع حياة الأفراد في خطر وينتهك حقهم في التمتع بحماية القانون (AMNESTY, 2020, p.13).

ولا يتفق الباحث مع استخدام مصطلح "المراقبة الحكومية" الذي يوحي برسمية وشرعية الإجراء وحوكمة الدولة له، إلا أن الجميع قد يتفق على أن هذه التجاوزات التقنية ـ أياً كانت الجهة التي تمارسها ـ تُمثل انتهاكاً صارخاً لحقوق الإنسان الرقمية؛ ففضلاً عن انطوائها على استغلال غير المشروع للتكنولوجيات الحديثة للاتصالات والمعلومات، تتعارض هذه الممارسات التعسفية مع جملة من الحقوق الرقمية كحق الإنسان في أن تُحترم خصوصيته وشؤون أسرته وبيته وعلاقاته ومراسلاته الخاصة، وحقه في سرية بياناته الشخصية، وحقه في حرية الاتصال والأنشطة السلمية وتكوين الجمعيات، وحقه في استخدام وسائل التكنولوجيا والبرمجيات والترددات اللاسلكية دون مراقبة أو مضايقة، وذلك على النحو المبين إجمالاً في المادة (١٢) من الإعلان العالمي لحقوق الإنسان والمادة (١٧) من العهد الدولي الخاص بالحقوق المدنية والسياسية.

ويتفق الباحث مع ما أنتهى إليه المنتدى الدولي للرقابة على الاستخبارات International Intelligence Oversight Forum الذي عقد في بوخارست عام ٢٠١٦ من أن مراقبة الاتصالات الرقمية يجب أن تكون متسقة مع الالتزامات الدولية المتصلة بحقوق الإنسان، وأن تتم بالاستناد إلى إطار قانوني معلن وواضح ودقيق وخال من التمييز، وأن أي مساس بالحقوق الرقمية يجب ألا يكون جماعياً أو تعسفياً أو غير قانوني، مع مراعاة المشروعية والضرورة والتناسب. وبهدف الحد من إساءة استخدام المراقبة على نطاق العالم وضمان أفضل الممارسات والضمانات في ميدان قضايا الأمن وانتهاك حقوق الإنسان الأساسية، والرقمية بصفة خاصة، أوصى المنتدى بضرورة سن صك قانوني دولي لتنظيم المراقبة الرقمية.

لا شك أن تحقيق التوازن بين الفعالية في مكافحة الجرائم الخطرة التي تهدد الأمن الوطني واحترام حقوق الإنسان الرقمية التي تشكل دعامة أساسية في العصر الرقمي تُعد من المسائل الشائكة والحساسة، لا سيما في الوطن العربي الذي تموج به الأخطار والتهديدات، إلا أن الباحث يرى أنه بالإمكان تحقيق المواءمة من خلال إخضاع المراقبة الرقمية وتكنولوجياتها التطبيقية للرقابة القضائية والإدارية الفعالة؛ فمتى دعت الحاجة الملحة إلى استخدام تقنيات المراقبة لضمان الأمن القومي ومباشرة التحقيقات الجنائية فإن استخدام سلطات الأمن لهذه

التقنيات والوسائل يجب أن يكون محاطاً بالضوابط والضمانات التشريعية التي تتوافق مع المصلحة العامة والثوابت الدولية بشأن حقوق الإنسان.

ومن المبادئ القضائية الدولية الهامة التي يمكن الاستئناس بها في هذا السياق، ما قررته محكمة العدل الأوروبية مؤخراً بأنه "في حين أن فاعلية مكافحة الجرائم الخطيرة، لا سيما الجريمة والمنظمة والإرهاب، يمكن أن يعتمد بدرجة كبيرة على تقنيات التحقيق والمراقبة الحديثة، فإن هذا الهدف الذي يمس المصلحة العامة، مهما كانت أهميته الجوهرية، لا يمكن في حد ذاته أن يُبرر اعتبار تشريع وطني ينص على الاحتفاظ بشكل عام وعشوائي بجميع بيانات حركة الاتصالات والمواقع ضرورياً لأغراض تلك المكافحة". وأكدت المحكمة بأن الاحتفاظ بالبيانات الرقمية ومراقبة حركة الاتصالات هو الاستثناء وليس القاعدة، ولا ينبغي اللجوء إليه إلا عندما تكون هناك دلائل ملموسة على ارتكاب جرائم خطيرة، وفي ظل وجود ضمانات وسبل انتصاف للأشخاص المشتبه بهم، وكذلك معايير مقيدة وآليات رقابة فعالة تشمل آليات للضبط (*Tele 2 Sverige AB v. Swedish Post & Telecom Authority*).

يتضح من هذا المبحث، أن العصر الرقمي الذي تعيشه البشرية حالياً وما أتاحه للأفراد من استخدام لامحدود لتكنولوجيات المعلومات والاتصالات الحديثة قد شابه انتهاكات للكثير من حقوق الإنسان الرقمية والخدمات الإنسانية المرتبطة بالإنترنت، مما أضر كثيراً بالاستقرار الأمني والسلام المجتمعي، وباعتبار الكوادر الشرطية هي المسؤولة عن حماية الأمن والسكينة في المجتمع، فإن التصدي بفعالية للتحديات المرتبطة بالحقوق الرقمية في سياق تكنولوجيا الاتصالات والتقنيات الذكية، سيتطلب العمل الأمني المتواصل والمتضافر لتحسين حماية حقوق الإنسان الرقمية في جميع أنحاء العالم العربي، الذي أضحى اليوم وأكثر من أي وقت مضى مطالب بتأمين فضائه الرقمي واقتصاده الرقمي وتطوير الاستراتيجيات الوطنية والعربية المعززة لتسخير إمكانات وفرص الثورة الرقمية لخدمة الشعوب العربية.

المبحث الثالث
دور أجهزة الشرطة في حماية وتعزيز حقوق الإنسان الرقمية

تمهيد وتقسيم:

تعتمد مجتمعات العالم عموماً والمجتمعات العربية على وجه الخصوص على الشرطة في حمايتها وتحقيق الإنفاذ الفعال للقانون، وتعتمد كذلك وبشكل متزايد ـ كباقي شعوب العالم ـ على تكنولوجيا المعلومات والاتصالات الرقمية، وبتزايد المخاطر والتهديدات في البيئة الرقمية، يتزايد الاعتماد على الشرطة في القيام بدورها الأصيل في حماية الأمن والنظام العام، ليس فقط في المجالات التقليدية الثلاثة للسيادة الوطنية (وهي البر والبحر والجو)، وإنما مجال رابع جديد وهو الفضاء الرقمي، وما يكتنفه من انتهاكات وتجاوزات متعلقة بممارسة حقوق الإنسان الرقمية.

ويشير خبراء مركز Kaspersky للأمن الرقمي بأن التهديدات الرقمية المستقبلية ستزداد تعقيدًا وستكون أكثر تنوعاً وانتقائيةً مدفوعةً بالتطور التقني، لذلك شاع في الآونة الأخيرة مصطلح "أمننة" securitization البيئة الرقمية، والذي يفرض على الأجهزة الشرطية والأمنية مواكبة هذه التطورات والاستعداد لها بواسطة تدابير قانونية واستراتيجيات أمنية خاضعة لتطوير وتحسين مستمر. ويسعى هذا المبحث الأخير إلى مناقشة الأطر القانونية الدولية والوطنية ذات العلاقة بحماية حقوق الإنسان الرقمية، بالإضافة إلى تسليط الضوء على أفضل الممارسات والسياسات الإقليمية في مجال العمل الأمني والحقوق الرقمية، واستعراض أبرز المبادرات الشرطية العربية في هذا الشأن، وصولاً إلى تحليل نتائج استبيان قياس الوعي والجاهزية الرقمية للكوادر الشرطية العربية، كل ذلك من خلال أربعة مطالب كما يلي.

المطلب الأول
الأطر القانونية الدولية والوطنية المساندة لدور الشرطة في حماية حقوق الإنسان الرقمية

تُوصف الشرطة بأنها "سلطة إنفاذ قانون"؛ فهي أداة الدولة الأساسية في تنفيذ القوانين، ولما كانت القوانين هي أهم الوسائل في حماية حقوق الإنسان، فإنه يستلزم أولاً التأسيس لأعمال الشرطة في هذا المضمار بمنظومة تشريعية متينة، ثم يتوجب على الشرطة تحقيق الإنفاذ الفعال لتلك القوانين، وخصوصاً الجنائية، فبقدر ما تقوم الكوادر الشرطية بتطبيق قوانين حقوق الإنسان بحرفية ومشروعية، فإنها تساهم بشكل كبير في حماية حقوق الإنسان وحرياته الأساسية. لذلك، تعتبر الشرطة حلقة هامة في منظومة العدالة الجنائية وحماية حقوق الإنسان المختلفة، وهي بالفعل خط الدفاع الأول في حماية حقوق الإنسان الرقمية.

ولعل المصدر الدولي الرئيسي للسلطة التي تستند إليها الشرطة في إنفاذ وفرض احترام القوانين المتعلقة بحقوق الإنسان هو الإعلان العالمي لحقوق الإنسان UDHR، وقد سبقت الإشارة إلى أن هذه الوثيقة الأممية

الملزمة التي مضى على صدورها أكثر من نصف قرن لم تنص صراحةً على الحقوق الرقمية حديثة النشأة، إلا أن نصوص الوثيقة التي تتضمن المعايير الدولية لحقوق الإنسان قد صيغت بلغة عامة وعريضة لتستوعب المستجدات المستقبلية في هذا الميدان الرحب. فالمادة (٣) من الإعلان تنص على أنه "لكل فرد الحق في الحياة والحرية وفي الأمان على شخصه"، وتنص المادة (١٢) على أنه "لا يجوز تعريض أحد لتدخل تعسفي في حياته الخاصة أو في شؤون أسرته أو مسكنه أو مراسلاته، ولا لحملات تمس شرفه وسمعته. ولكل شخص حق في أن يحميه القانون من مثل ذلك التدخل أو تلك الحملات". ولما كان انتهاك حقوق الإنسان الرقمية يتضمن في حقيقته مساس بحرية الأفراد وأمنهم، ويشكل كذلك تدخل تعسفي في شؤون الحياة الخاصة والمراسلات الرقمية، فإن الشرطة ملزمة بإنفاذ هذه النصوص الدولية ـ التي تعتبر جزءً من التشريع الوطني ـ وتوفير حماية قانونية لأصحاب الحقوق الرقمية. لذلك، لا غرو في أن يشير الدليل الذي أعدته مفوضية الأمم المتحدة لحقوق الإنسان لتدريب الشرطة على حقوق الإنسان وإنفاذ القانون إلى أن "نص الإعلان العالمي لحقوق الإنسان هو برمته توجيه لعمل الشرطة" (OHCHR, Human rights standards & practice for police, p.29).

ومن الصكوك الدولية التي تشكل إطار قانوني هام لعمل الشرطة في مجال حقوق الإنسان، مدونة قواعد سلوك الموظفين المكلفين بإنفاذ القوانين التي اعتمدت بموجب قرار الجمعية العامة للأمم المتحدة رقم (٣٤/١٦٩) لسنة ١٩٧٩، حيث نصت المادة (١) من المدونة بأنه "على الموظفين المكلفين بإنفاذ القوانين، في جميع الأوقات، أن يؤدوا الواجب الذي يلقيه القانون على عاتقهم، وذلك بخدمة المجتمع وبحماية جميع الأشخاص من الأعمال غير القانونية، على نحو يتفق مع علو درجة المسؤولية التي تتطلبها مهنتهم". وأكدت المادة (٢) على أن "يحترم الموظفون المكلفون بإنفاذ القوانين، أثناء قيامهم بواجباتهم، الكرامة الإنسانية ويحمونها، ويحافظون على حقوق الإنسان لكل الأشخاص ويوطدونها". مما يعني واجب منتسبي الشرطة باحترام حقوق الإنسان والدفاع عنها دوماً، ولا يقتصر هذا الواجب على التشريعات المحلية ولكن أيضاً معايير حقوق الإنسان المقررة دولياً، بما فيها الحقوق الرقمية كونها متصلة بالكرامة الإنسانية.

والحقيقة أن الشرطة باعتبارها جهاز فاعل من أجهزة الدولة، وإحدى وسائلها في تنظيم المجتمع عن طريق ما يفرضه المشرع من قوانين وأنظمة، تُلزم بعض الوثائق الدولية "الدولة" the State ـ في المقام الأول ـ برعاية حقوق الإنسان وحرياته الأساسية. فقد نص ميثاق الحقوق الرقمية الأساسية للاتحاد الأوروبي في ديباجته صراحةً على مسؤولية الدولة في حماية الحقوق الأساسية لمواطنيها، مع خضوع ممارسات الدولة لمسؤوليتها الحقوقية لقيود دستورية صارمة. وتنص المادة (٣) من الميثاق العربي لحقوق الإنسان على أن تتعهد كل دولة بأن تكفل لكل شخص خاضع لولايتها حق التمتع بالحقوق والحريات المنصوص عليها قانوناً، وتتخذ في سبيل ذلك التدابير اللازمة لتأمين تمتع الجميع بكافة حقوق الإنسان.

وتتصدر الدساتير constitutions قمة التشريعات الوطنية في إقرار المعايير الدولية بشأن حقوق الإنسان، حيث أفردت معظم الدساتير العربية قواعد كلية لأهم الحقوق والحريات الأساسية كالحق في الأمن والحق في حرمة الحياة الخاصة والحق في سرية المراسلات والاتصالات، بالإضافة إلى انضمام عدد كبير من الدول العربية للعهدين الدوليين، وبالتالي إندماج المبادئ الواردة بهما في القوانين المحلية. وبمراجعة بعض الدساتير العربية تلاحظ خلوها من نصوص صريحة تحمي حقوق الإنسان الرقمية، بإستثناء مادة وحيدة في الدستور المصري المعدل سنة ٢٠١٩، وهي المادة (٣١) التي تشير إلى أن "أمن الفضاء المعلوماتي جزء أساسي من منظومة الاقتصاد والأمن القومي، وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه، على النحو الذي ينظمه القانون". كما تنص المادة (٤٠) من الدستور العراقي الصادر عام ٢٠٠٥ على أن "حرية الاتصالات والمراسلات البريدية والبرقية والهاتفية والالكترونية وغيرها مكفولة، ولا يجوز مراقبتها أو التنصت عليها، أو الكشف عنها، إلا لضرورة قانونية وأمنية، وبقرار قضائي".

وبالمقارنة، أورد الدستور الإسباني المعدل سنة ٢٠١٨ (Spanish Constitution Law 3/2018) فصولاً خاصة بحماية البيانات الشخصية وضمان الحقوق الرقمية؛ فلم تجز المادة (٣٨) منه "جمع أي بيانات شخصية للمستخدمين أو نقلها إلى طرف ثالث في البيئة الرقمية دون موافقتهم أو علمهم"، ووفرت المادة (٨٧) حماية خاصة للحق في الخصوصية الرقمية ضد استخدام برامج المراقبة بالفيديو وأجهزة التسجيل الصوتي وأنظمة تحديد الموقع الجغرافي وغيرها. وتتوافق هذه النصوص الدستورية مع قانون الإتحاد الأوروبي رقم (٢٠١٦/٦٧٩) بشأن حماية البيانات الشخصية الرقمية، الذي اشتمل على ٩٩ مادة قانونية مفصلة في الموضوع، من بينها فصل خاص بقواعد سلوك ممارسة الرقابة الأمنية عبر التقنيات الرقمية.

لا شك أن هذه المعايير والضوابط الدستورية توفر ضمانات للأفراد وتفرض قيوداً على جميع السلطات، إلا أنه وبالرغم من سموها وعلوها على بقية التشريعات، فهي ليست النصوص الوحيدة التي يجب الالتزام بها وعدم مخالفتها. فمن جانب آخر، نجد بعض قوانين العقوبات الحديثة تفرد نصوصاً ذات علاقة بحماية حقوق الإنسان الرقمية، فعلى سبيل المثال، تنص المواد (٣٧١ - ٣٨٧) من قانون العقوبات القطري لسنة ٢٠٠٤، على تجريم الدخول غير المشروع على أنظمة الحاسب الآلي، وأفعال الإتلاف المعلوماتي أو المادي للحاسبات الآلية، وممارسات الإجرام الفيروسي والتزوير أو الاحتيال المعلوماتي. كما تنص المادة (٣٠٩) مكرراً (١) من قانون العقوبات المصري المعدل سنة ٢٠٠٣ على عقاب "كل من اعتدى على حرمة الحياة الخاصة للمواطن، وذلك بأن إرتكب أحد الأفعال الآتية في غير الأحوال المصرح بها قانوناً أو بغير رضاء المجني عليه. (أ) استرق السمع أو سجل أو نقل عن طريق جهاز من الأجهزة أياً كان نوعه محادثات جرت في مكان خاص أو عن طريق التليفون. (ب) التقط أو نقل بجهاز من الأجهزة أياً كان نوعه صورة شخص في مكان

خاص". من الواضح أن هذا النص ليس خاصاً بالاتصالات الرقمية أو الصور الإلكترونية، ولكنه قد يشملها بمفهومها العام، وذلك لاتحاد المحادثات الهاتفية مع الرقمية في الجوهر وإن اختلفا في الشكل.

وتتضمن الترسانة التشريعية العربية كذلك العديد من القوانين الجنائية الخاصة بمكافحة جرائم الحاسب الآلي أو تقنية المعلومات أو الجرائم المعلوماتية، وقوانين أخرى خاصة بتنظيم الاتصالات، والمعاملات الإلكترونية، والتجارة الإلكترونية، والدفاع الإلكتروني، وتهدف هذه القوانين في مجملها إلى تحقيق السلامة المعلوماتية من خلال منع استخدام الحاسب الآلي أو شبكات الاتصالات للتعدي على سلامة وسرية وتوافر البيانات والمعلومات الإلكترونية والنظم المعلوماتية، وهي بذلك تشكل إطاراً قانونياً عاماً لحماية الحقوق الرقمية، إلا أنها تظل غير كافية؛ نظراً للطبيعة الخاصة والمتنامية لحقوق الإنسان الرقمية، وهو ما أدركته التشريعات الأوروبية، وسنت تشريعات حديثة خاصة بحماية الهوية الرقمية والخصوصية الرقمية في الفضاء الرقمي.

وقد أفاد ١٥,٥٪ من رجال الشرطة العرب المجيبين على الاستبيان المستخدم بهذه الدراسة بأن مؤسساتهم الشرطية لا تطبق قوانين جنائية أو تشريعات إدارية خاصة بالرقابة على احترام حقوق الإنسان الرقمية، كما أن ٢٦,٢٪ غير متأكدين من وجود تشريعات في هذا الجانب، مما يدلل على وجود نقص تشريعي وعدم اكتمال الأطر التشريعية في هذا الجانب بشكلٍ كامل. ولعل هذا ما دفع لجنة الأمم المتحدة الاقتصادية والاجتماعية لغرب آسيا UN Economic & Social Commission for Western Asia (ESCWA) على التشديد في وقت سابق بضرورة أن تتضمن التشريعات العربية الرقمية أحكام خاصة بمكافحة الاعتداءات الرقمية وتعزيز الأمن الرقمي.

بناءً عليه، يرى الباحث أهمية أن تتضمن الدساتير والقوانين العربية نصوصاً خاصة وصريحة تكفل الحماية الكاملة للحقوق الرقمية، وذلك سواء بتعديل التشريعات القائمة لجعلها أكثر ملائمةً، أو بإستحداث تشريعات جديدة قادرة على مواكبة الأهمية والتطور المتسارع الذي تشهده حقوق الإنسان الرقمية. فالتشريعات السليمة المواكبة للتطورات الرقمية هي الأساس التشريعي الذي يلزم جميع السلطات في الدولة باحترام هذه الحقوق وحمايتها، وكذلك السند القانوني الذي تستند إليه الكوادر الشرطية في مكافحة الانتهاكات التي تتعرض لها الحقوق الرقمية وملاحقتها قضائياً، لذلك يجب دائماً أن تتسم الإجراءات الشرطية في المحافظة على حقوق الإنسان الرقمية بالشرعية الإجرائية والموضوعية معاً.

المطلب الثاني
جهود ومبادرات أجهزة الشرطة الدولية والإقليمية في حماية وتعزيز حقوق الإنسان الرقمية

لقد تنبهت الكثير من أجهزة الشرطة حول العالم لصعوبة التمسك بذات الأطر القانونية التقليدية والإجراءات التنظيمية المعتادة في العصر الرقمي والتقدم التقني الذي يعيشه العالم اليوم، كما أدركت بأن دورها في حماية حقوق الإنسان الرقمية لا يقتصر على مكافحة الجرائم الرقمية فقط، بل يتعداه إلى تعزيز ممارسة هذه الحقوق، فبادرت ـ وبشكل مبكر ـ إلى استحداث خدمات شرطية حديثة وأجهزة رقمية متخصصة لمواكبة التحول المجتمعي الرقمي societal digital transformation الذي يتطلب حضور أكبر وأكثر تأثيراً للشرطة في الفضاء الرقمي. ويعول الدليل العالمي للأمن السيبراني على المعايير التنظيمية organizational pillar كإحدى الركائز الرئيسية لتقييم أداء الدول في مجال الأمن السيبراني أو الرقمي، وتقاس البنى التنظيمية ـ وفقاً للدليل ـ على أساس مدى وجود مؤسسات واستراتيجيات لتنسيق سياسات تطوير الأمن الرقمي على المستوى الوطني (GCI, 2020). بينما يؤكد مؤتمر ميونيخ للأمن لعام ٢٠٢١ على حتمية التعاون الرقمي والتنسيق الأمني لمواجهة التحديات التقنية و "العدوان الكبير الذي تتعرض له الثقة الرقمية" digital distrust (Munich Security Report 2021, p.33).

وقد أثمرت الجهود الدولية والإقليمية الأخيرة عن ظهور مصطلح "الشرطة الرقمية" digital police، والذي جاء استجابةً للواقع الرقمي الحالي الغير مسبوق؛ حيث الاعتماد الكامل والدائم على تقنيات المعلومات والاتصالات، ودخول البرمجيات الرقمية في أدق تفاصيل حياة الأفراد الشخصية، كنتيجة للترابط الرقمي العالمي، مما فرض على أجهزة الشرطة مسايرة هذا التطور، والتحول إلى شرطة رقمية لخدمة وحماية المجتمع الرقمي. ففي المؤتمر الدولي الأول لـ "تحديات الأمن الرقمي" الذي عقدته منظمة الإنتربول في عام ٢٠١٦ بسنغافورة، تم التأكيد على أنه "في العالم الرقمي الذي أدى إلى ظهور حاجات مجتمعية جديدة وأفرز جرائم رقمية متغيرة، تُعد القدرات الرقمية الشرطية مكوناً أساسياً للشرطة العصرية الناجحة"، وكمبادرة على إلتزام المنظمة الدولية للشرطة الجنائية ببناء وتحسين المهارات الرقمية للمحققين الجنائيين في جميع أنحاء العالم، تم إنشاء مركزي "التواصل والابتكار الرقمي"، ومركز "مكافحة الجرائم الإلكترونية" التابعين للإنتربول (INTERPOL, Digital Security Challenge 2016).

وعلى المستوى الإقليمي، أدرجت منظمة الشرطة الأوربية Europol موضوع "الشرطة الرقمية" و "رقمنة الأجهزة الأمنية" digitization of the security authorities في صدارة موضوعات مؤتمر الشرطة الأوروبي لعام ٢٠٢٠، حيث أكد المؤتمر على ضرورة الإسراع في تنفيذ توصيات "المؤتمر الثالث للجرائم الإلكترونية" الذي عُقد في عام ٢٠١٦ بالشراكة مع الإنتربول حول رقمنة الخدمات الشرطية وزيادة التعاون الرقمي بين السلطات الأمنية الأوروبية لجعل الحقوق الرقمية في مأمن من كافة الاعتداءات. كما تم إطلاق

"وحدة الشرطة الأوروبية للتحريات والتحقيقات الرقمية" (EU-IRU)، التي تضم مجموعة من المختصين في التقنيات الرقمية وتكنولوجيا المعلومات والاتصالات، وتختص بكشف المحتوى الضار على الإنترنت وشبكات التواصل الاجتماعي والتحقيق فيه، بالإضافة إلى تقديم الدعم الرقمي لكافة أجهزة الشرطة بالاتحاد الأوروبي من خلال توفير التحليل الاستراتيجي والتشغيلي (European Police Congress 2020).

وترجمةً لهذه السياسات الأوروبية الشرطية بشأن التحول الرقمي في العمل الأمني، سارعت كلاً من المانيا وهولندا والنمسا وبلجيكا والسويد والنرويج والبرتغال وإسبانيا إلى إنشاء إدارة للتطوير الرقمي Digital Director ضمن هيكل وزارة الداخلية، تولت تبني نماذج حديثة للشرطة الرقمية وإدخال خدمات رقمية جديدة للعمل الشرطي كمختبرات الأدلة الرقمية وتقديم البلاغات والشكاوى عبر الإنترنت. بينما شكلت فرنسا فريقاً مختصاً من الخبراء (French acronym GTTSI) لتسريع استيعاب الشرطة للتقدم التكنولوجي والابتكارات الرقمية، وقد تمخض عن ذلك توسع الشرطة الفرنسية في تقديم خدماتها العامة عبر الإنترنت، وتزويد منتسبي الشرطة بمجموعة متطورة من معدات التدخل التقنية التي تسمح بتجوال قواعد البيانات وتبادل المعلومات والمعارف، بالإضافة إلى توظيف طائرات الدرونز في التوعية الأمنية وضبط المخالفين، واستخدام تقنيات الذكاء الاصطناعي والبيانات الضخمة في التحقيقات الجنائية وحماية الحقوق الرقمية. ويمكن القول بأن هذه التطورات الرقمية مستمدة من الرؤية الرقمية للشرطة الفرنسية digital vision في "أن تصبح - من خلال استخدام التقنيات الرقمية – إحدى أول ثلاث قوى أمنية رائدة في العالم من حيث الكفاءة وجودة الخدمة المقدمة للمجتمع".

ويرى الباحث بأن المبادرة البريطانية British policing model هي التجربة الأبرز والأشمل في مجال حماية وتعزيز حقوق الإنسان الرقمية، حيث تبنت الشرطة البريطانية مؤخراً "استراتيجية مستقبلية رقمية ٢٠٢٥" Police Digital, Data and Technology Strategy 2025 تقوم على خمسة محاور رئيسية وهي: ١- تسهيل التواصل بين الشرطة والجمهور من خلال خدمات رقمية سلسة؛ ٢- تسخير التكنولوجيا الرقمية لمكافحة الانتهاكات الرقمية وتقديم نُهج شرطية استباقية أكثر دقة وانتقائية؛ ٣- تزويد الكوادر الشرطية بالقدرات الرقمية المتقدمة لتحسين الأداء الجنائي ودعم العمليات الخطرة والأنشطة ذات القيمة المضافة؛ ٤- تعزيز سياسة الانفتاح الرقمي وزيادة التعاون مع الجهات الحكومية لمعالجة قضايا السلامة المعلوماتية وفق نظام عدالة جنائية فعال وشفاف؛ ٥- تعميق الشراكة المجتمعية ومشاركة مسؤوليات حماية السلامة الرقمية مع الجمهور والقطاع الخاص. وفي سبيل تطبيق هذه الرؤية الرقمية تم إنشاء أربع وحدات متخصصة وهي: ١- وحدة متابعة تنفيذ استراتيجية الشرطة الرقمية Digital Policing Portfolio (DPP)، ٢- وحدة التحريات والتحقيقات الرقمية Digital Intelligence and Investigation (DII)؛ ٣- وحدة تبادل المعلومات والأدلة الجنائية الرقمية Digital First (DF)؛ ٤- وحدة التواصل المجتمعي

الرقمي (UK Policing Vision 2025) Digital Public Contact (DPC). ولم تغفل الاستراتيجية بيان المعايير والمبادئ الأخلاقية التي ينبغي أن تتحلى بها الشرطة الرقمية؛ حيث نصت على أن واجبات الشرطة الحديثة في البيئة الرقمية يجب أن تستند إلى "مدونة الأخلاق الشرطية" Police Code of Ethics وأن تُرسخ مبادئ الشرعية والأمانة والثقة، وذلك تحت رقابة وإشراف اللجان الانضباطية المنصوص عليها في لائحة سلوك الشرطة لعام ٢٠١٢م وتعديلاتها Police (Conduct) Regulations 2012، ولائحة سوء السلوك والشكاوى ضد رجال الشرطة لعام ٢٠١٢م وتعديلاتها Police (Complaints and Misconduct) Regulations 2012.

يظهر من خلال هذا الاستعراض الموجز لبعض الجهود والآليات الشرطية الحديثة المستخدمة لتحقيق التحول الرقمي وحماية الحقوق الرقمية، أنه أصبح لزاماً على أجهزة الشرطة في العصر الرقمي وما أفرزه من حقوق ومخاطر رقمية مواكبة التطورات الدولية والمحلية من خلال تبني سياسات ومبادرات تساير ـ بل وتستبق ـ احتياجات المجتمع الرقمي. وهو ما أدركته أجهزة الشرطة الأوروبية، فلم تقف عند حد مكافحة انتهاكات حقوق الإنسان الرقمية وتأمين سلامة الأفراد في الفضاء الرقمي، وإنما عملت على تقديم خدمات رقمية متنوعة تصب في مجال تعزيز ممارسة الحقوق الرقمية وتلبي رضا وتطلعات مجتمعاتها.

المطلب الثالث
جهود أجهزة الشرطة العربية في حماية وتعزيز حقوق الإنسان الرقمية

بخلاف القفزات الرقمية التي حققتها أجهزة الشرطة الأوروبية في مجال حماية وتعزيز حقوق الإنسان الرقمية، تبذل معظم أجهزة الشرطة العربية جهوداً متواضعة بعض الشيء في هذا المجال الحيوي، وذلك بالرغم من تغلغل تكنولوجيا المعلومات والاتصالات في حياة المجتمعات العربية، التي تعتبر من أكثر المجتمعات في العالم امتلاكاً للهواتف الذكية واستخداماً للأنترنت (GCI,2020). وتشير التقارير الدولية المتخصصة إلى تعرض الدول العربية لملايين الهجمات والاعتداءات الرقمية، وبنسب تفوق مثيلاتها في جميع أنحاء العالم (Kaspersky, Digital Dangerscape, 2020). وقد يكون هذا الاستهداف الرقمي للدول العربية راجعاً إلى عدم فعالية السياسات الأمنية والأطر التشريعية بالقدر الكافي لمواجهة الهجمات الرقمية، بالإضافة إلى ضعف الضوابط الحمائية والإجراءات الدفاعية، والبطء في استخدام تقنيات حماية الأمن الرقمي لأسباب اقتصادية وتقنية (The Economist Intelligence Unit, 2018).

ويشدد تقرير حقوق الإنسان في الوطن العربي لعام ٢٠١٨ على أن أبرز الانتهاكات الرقمية التي شهدتها البلدان العربية تمثلت في انتهاكات شبكة الإنترنت ووسائل التواصل الاجتماعي، وانتهاكات الصحافة الإلكترونية، الأمر الذي يشكل تهديداً جدياً لمنظومة الأمن العربي المشتركة، ويستدعي التدخل الفوري

للحكومات العربية والأجهزة الأمنية لحماية هذه الحقوق الأساسية، مع أهمية دمج حقوق الإنسان في أهداف التنمية المستدامة، وبالشراكة مع المجتمع المدني، وعبر نُهج أكثر شمولاً (تقرير حقوق الإنسان في الوطن العربي، ٢٠١٨، ص ٤٥، ٢٥٧).

ويبدو أن اختيار المركز العربي للدراسات الأمنية والتدريب بالرياض لموضوع "الشرطة وحقوق الإنسان" كموضوع لأحد الندوات العلمية التي نظمها في عام ١٩٩٥ كان اختياراً مبكراً يدل على سعة أفق وبُعد نظر بشأن طبيعة التحديات المستقبلية التي سوف تواجه العمل الأمني. وتأكيداً على تعاظم أهمية الموضوع في الزمن الرقمي المعاصر، عُقد بالدوحة في نهاية عام ٢٠١٤ وبالتعاون مع مجلس وزراء الداخلية العرب مؤتمر دولي خاص بشأن "تحديات الأمن وحقوق الإنسان في المنطقة العربية"، حيث سلط المؤتمر الضوء على أهمية الشراكة بين الأجهزة الأمنية والمؤسسات الوطنية لحقوق الإنسان من أجل تعزيز احترام حقوق الإنسان إجمالاً، مع التأكيد على أن ضمان الأمن واحترام حقوق الإنسان هما مسؤوليتين أساسيتين من مسؤوليات الدول.

وعلى الرغم من عدم تطرق هذا المؤتمر لقضايا حقوق الإنسان الرقمية في العمل الأمني كموضوع معاصر تنبهت إليه أجهزة الشرطة المعاصرة، إلا أن النسخة الثانية من هذا المؤتمر التي عقدت بتونس عام ٢٠١٥ كلفت الأمانة العامة لمجلس وزراء الداخلية العرب بإعداد خطة عمل استرشادية للأجهزة الأمنية في مجال حماية حقوق الإنسان المعاصرة، إلا الباحث لم يُوفق في العثور على نسخة من هذه الخطة. ويرى الباحث بأن "المؤتمر السادس للمسؤولين عن حقوق الإنسان في وزارات الداخلية العربية" الذي انعقد مؤخراً في فبراير من هذا العام عبر تقنية الاتصال المرئي، كان أكثر إنتاجيةً ومساهمةً في هذا المجال؛ إذ أوصى بتشكيل المزيد من الهياكل الرقابية على احترام حقوق الإنسان ضمن الأجهزة الأمنية، وإنشاء موقع إلكتروني خاص بإدارات حقوق الإنسان في وزارات الداخلية العربية، وكذلك تكليف الدول الأعضاء بتقديم تقرير سنوي يعرض تجاربها في مجال حقوق الإنسان، على أن يتضمن قسم خاص بحالات انتهاك حقوق الإنسان من قبل الأجهزة الأمنية إن وجدت.

ومن التجارب الوطنية الجيدة التي تُظهر جهود أجهزة الشرطة العربية في حماية حقوق الإنسان ومن بينها الحقوق الرقمية، تجربة شرطة دبي بدولة الإمارات العربية المتحدة، والتي أنشأت في عام ١٩٩٨ إدارة خاصة ضمن هيكل شرطة دبي بمسمى "الإدارة العامة لحقوق الإنسان"، تختص بالتحقيق في الشكاوى المقدمة ضد انتهاكات حقوق الإنسان وضمان الاحترام الكامل لحقوق الإنسان وحرياته في العمل الشرطي، حيث تتلقى الإدارة في العام الواحد مئات الشكاوى، وهو ما يعزز "سبل الانتصاف المحلية الفعالة" التي نادت بها المواثيق الدولية. كما تم في عام ٢٠١٩ إطلاق "الاستراتيجية الوطنية للأمن الرقمي"، والتي تسعى إلى حماية أفراد المجتمع ضد الهجمات الرقمية وحماية البيانات الشخصية الحساسة التي هي من صميم الحقوق الرقمية، وقد

تمخض عن هذه الاستراتيجية الرقمية إنشاء "النيابة الاتحادية لجرائم تقنية المعلومات"، ومراكز شرطة ذكية، بالإضافة إلى تقديم خدمات رقمية متطورة كخدمة تبادل معلومات مع الشرطة، وخدمة البلاغات العامة، وخدمة الإبلاغ عن حادث ضد مجهول، وخدمة الدعم ضد الجرائم الإلكترونية، وذلك عبر الموقع الإلكتروني للشرطة (www.dubaipolice.gov.ae).

وفي نهج آخر متطور، استحدثت سلطنة عُمان في عام ٢٠٢٠ "مركز الدفاع الإلكتروني" الذي يتبع جهاز الأمن الداخلي، ويهدف إلى بناء القدرات الوطنية في مجال الأمن الرقمي وتعزيز قدرات الجهات الأمنية والأفراد على التصدي للاعتداءات الرقمية. كما يضطلع "المركز الوطني للسلامة المعلوماتية" وبالتعاون مع "المركز العربي الإقليمي للأمن السيبراني" الذي تحتضنه السلطنة بتنفيذ "إستراتيجية عُمان الرقمية ٢٠٣٠"، التي وفرت بدورها مظلة لجهاز شرطة عُمان السلطانية للمضي قدماً في التحول الرقمي ونشر الثقة والأمن في إستخدام تكنولوجيا المعلومات والاتصالات من خلال تسجيل حضور أمني قوي في البيئة الرقمية عبر مواقع إلكترونية شرطية، وتدشين خدمات رقمية متعددة تُمكن الجمهور من ممارسة حقوقهم الرقمية بدون عقبات (www.rop.gov.om).

كما تُعد مديرية الأمن العام بالمملكة الأردنية الهاشمية إحدى النماذج الرائدة بالمنطقة في مجال رعاية حقوق الإنسان، حيث أسست منذ عام ٢٠٠٥ "مكتب الشفافية وحقوق الإنسان"، الذي يختص بالتحقيق في التجاوزات أو الممارسات الخاطئة الماسة بحقوق الإنسان التي تُنسب لرجال الشرطة، وكذلك مراقبة إلتزام العمل الشرطي بالمعايير الدولية لحقوق الإنسان، ويتبع المكتب مركز تدريب متخصص في التوعية بحقوق الإنسان، يصلح لأن يكون مركز إقليمي يقدم خدماته لأجهزة الشرطة العربية. ومن الملفت للنظر أن المديرية وقعت مذكرات تفاهم مع المركز الوطني لحقوق الإنسان ونقابة المحامين وغيرها من المؤسسات المعنية بحقوق الإنسان لإجراء جولات تفتيشية مشتركة، وهو ما يعكس تبني سياسة الشراكة المجتمعية.

وتبذل أجهزة الشرطة في كلاً من مصر والسعودية وقطر والكويت والمغرب والجزائر جهوداً حثيثة للارتقاء بقدراتها الرقمية في مجال حقوق الإنسان، لا يسع المجال المخصص لهذا البحث لاستعراضها جميعاً، إلا أنه يمكن الاستفادة من التجارب العربية الأربعة المذكورة لتعزيز حقوق الإنسان الرقمية في العمل الأمني، حيث وصف الدليل العالمي للأمن السيبراني لعام ٢٠١٨ بعض دول الخليج العربي بأن لديها هياكل تنظيمية قوية لتعزيز أمنها الرقمي (GCI, 2018). من جانب آخر، يشير الدليل الصادر في عام ٢٠١٧ إلى وجود العديد من الثغرات في المعايير القانونية التنظيمية التي ينبغي على بعض الدول العربية معالجتها من خلال إتخاذ إجراءات لتطوير التشريعات وتحسين الأداء في البيئة الرقمية (GCI, 2017). كما يؤكد البرنامج العالمي

للأمن السيبراني (GCA) على أهمية تبني تدابير قانونية وهياكل تنظيمية تمكن السلطات المختصة من تأمين الفضاء السيبراني وحماية الحقوق الرقمية على نحو فعال.

وفي هذا المقام، لا بد من الإشارة إلى أن غالبية الدول العربية ـ بما فيها دول الخليج ـ وبالرغم من الرغبة الرسمية والإرادة السياسية، لم تتمكن بعد من رقمنة الأجهزة الأمنية وتطبيق مفهوم الشرطة الرقمية على أرض الواقع، بما يعزز حقوق الإنسان الرقمية ويلبي مطالب الرأي العام وحركة حقوق الإنسان في العالم العربي. وتظهر مواطن القصور في غياب الاستراتيجيات الرقمية بعيدة المدى للأجهزة الأمنية، وبالنسبة للدول التي تمتلك استراتيجيات عامة فإنه لا ينبغي وضع خطط وأهداف ومن ثم إهمال تطبيقها أو عدم إلزام الجهات المعنية بتنفيذ البنود والأحكام الواردة فيها. كما يُلاحظ غياب التنسيق الفعال والعمل المشترك بين أجهزة الشرطة العربية، بالرغم من أن مؤتمرات المسؤولين عن حقوق الإنسان في وزارات الداخلية العربية قد ناقشت في اجتماعاتها أهمية تبادل معلومات والتجارب وأفضل الممارسات في قضايا حقوق الإنسان ذات العلاقة بالعمل الأمني.

ومن الأمثلة الأخرى على ضعف التنسيق والتعاون في هذا المجال، أنه لم يجري حتى الآن عقد مؤتمر أو ندوة عربية حول حماية حقوق الإنسان الرقمية، كما أن التدريب الوحيد في مجال حقوق الإنسان على مستوى الدول العربية هو الذي نظمته جامعة نايف العربية للعلوم الأمنية في الرياض عام ٢٠١٣. لذلك، لا غرابة في اتساع الفجوة الرقمية بين الأجهزة الأمنية العربية وتمسك معظمها بالأساليب التقليدية في التعامل مع المجتمع الرقمي. وقد كشف الاستبيان المستخدم في هذه الدراسة ـ والذي شمل أغلب الدول العربية ـ إلى أن ١٧,٩٪ من رجال الشرطة العرب المجيبون على الاستبيان لا يعتقدون و١٧,٩٪ غير متأكدون بأن مؤسساتهم مواكبة للتطورات الرقمية بالمجتمع ومستعدة للتعامل معها، مما يشير إلى عدم اكتمال جاهزية أجهزة الشرطة العربية لمواكبة متطلبات وتحديات العصر الرقمي بشكلٍ يرضي ويتماشى مع طموحات وتطلعات شعوبها.

المطلب الرابع
نتائج استبيان قياس وعي وجاهزية الكوادر الشرطية العربية للتعامل مع قضايا حقوق الإنسان الرقمية

يُعتبر الاستبيان من أهم الوسائل المستخدمة في الأبحاث الأمنية، ويتضمن هذا المطلب الأخير استعراض وتحليل لردود رجال الشرطة العرب المشاركون في الاستبيان المستخدم بهذه الدراسة، بدايةً من توضيح موجز لبعض المعلومات عن تصميم الاستبيان، وأهدافه، ورجال الشرطة المشاركون به، وأجهزة الشرطة العربية المستجيبة له، ثم التحليل النقدي والإحصائي لنتائجه. ففيما يتعلق بتصميم الاستبيان، فقد تم بجهود الباحث مع استشارة كلاً من المركز العربي الإقليمي للأمن السيبراني التابع للاتحاد الدولي للاتصالات ITU والمسؤول عن المنطقة العربية، والشبكة العربية للمؤسسات الوطنية لحقوق الإنسان. وأما أهداف الاستبيان فقد تم تفصيلها بديباجة الاستبانة المرفقة بالملحق.

وقد استهدف الاستبيان مختلف الكوادر الشرطية بالدول العربية من ضباط وأفراد، حيث تم إرسال الاستبيان في يوليو ٢٠٢١م إلى منتسبي الشرطة بجميع الدول العربية، وذلك عبر تعاون وتنسيق المكاتب المركزية الوطنية للشرطة العربية (الإنتربول). وقد استجاب للاستبيان ما مجموعه (٨٤) أربعة وثمانون رجل شرطة، ينتمون لـ (١٦) ستة عشر دولة عربية، بحسب ما يوضح الجدول أدناه:

	أجهزة الشرطة العربية المستجيبـــــة								
الدولــة	الأردن	الإمارات	البحرين	جزر القمر	جيبوتي	السودان	العراق	عُمان	المجموع
العـــدد	٨	١٠	٣	١	٢	٧	١	٢٣	١٦ دولة
الدولــة	قطر	الكويت	لبنان	ليبيا	مصر	المغرب	السعودية	اليمن	المجموع
العـــدد	٣	١٢	٢	٣	٢	١	٣	٣	٨٤ مشارك

وقد كانت المؤهلات العلمية لرجال الشرطة المشاركين في الاستبيان متنوعة على النحو التالي: دكتوراه (١٤,٣٪)، ماجستير (٢٦,٢٪)، بكالوريوس (٣٦,٩٪)، دبلوم (١٠,٧٪)، ثانوية عامة (١١,٩٪)، ما دون الثانوية العامة (١٤,٣٪). وتعكس هذه المؤهلات مستويات علمية عالية، وهو ما يفترض دعمه تنفيذ قوانين حقوق الإنسان. وبتحليل الردود الواردة على أسئلة الاستبيان حول وعي وجاهزية الكوادر الشرطية العربية للتعامل مع قضايا حقوق الإنسان الرقمية، يتضح الآتي:

أولاً: الجانب المعرفي والثقافي المتصل بحقوق الإنسان الرقمية في العمل الشرطي:

السـؤال رقم (١)	نعم	لا	غير متأكد	المتوسط الحسابي	الانحراف المعياري	معامل الاختلاف
هل لديك إلمام ومعرفة بطبيعة وأنواع حقوق الإنسان الرقمية؟	٤٧,٦	٢٨,٦	٢٣,٨	٢,١٩	٠,٨٥	٣٨,٨٩

السـؤال رقم (٤)	نعم	لا	غير متأكد	المتوسط الحسابي	الانحراف المعياري	معامل الاختلاف
هل تلقيت تدريباً للتوعية بحقوق الإنسان الرقمية؟	١٧,٩	٧٥,٠	٧,١	١,٤٣	٠,٧٨	٥٤,٣١

يُلاحظ أولاً من الردود الواردة على السؤال الأول أن (٢٨,٦٪) من المشاركين ليس لديهم إلمام بحقوق الإنسان الرقمية، و (٢٣,٨٪) غير متأكدين من معرفتهم بهذه الحقوق، وكلا الرقمين يشكلا في حقيقة الأمر نسبة كبيرة بالمقارنة مع (٤٧,٦٪) فقط من المشاركين الذين لديهم إلمام بالحقوق الرقمية. كما أن الردود على السؤال الرابع تُظهر أنه باستثناء (١٧,٩٪) فقط، فإن الغالبية العظمى من المشاركين لم يتلقوا تدريباً للتوعية بحقوق الإنسان الرقمية، وهو ما يدلل في مجموعه على وجود نقص كبير في وعي الكوادر الشرطية العربية بحقوق الإنسان الرقمية، مما يتطلب تكثيف الجهود في هذا المجال، لأن الجهل بهذه الحقوق يعني عدم إمكانية حمايتها بشكل صحيح، بل ومخالفتها أو انتهاكها نتيجةً لعدم الإلمام بها.

ثانياً: الجانب المؤسسي والتنظيمي المتصل بحقوق الإنسان الرقمية في العمل الشرطي:

السـؤال رقم (٢)	نعم	لا	غير متأكد	المتوسط الحسابي	الانحراف المعياري	معامل الاختلاف
هل يوجد بالمؤسسة إدارة أو قسم معني بحقوق الإنسان الرقمية؟	٢٩,٨	٥٢,٤	١٧,٩	١,٧٧	٠,٨٨	٤٩,٤٨

يتبين من الردود الواردة على السؤال الثاني أن نسبة كبيرة من وزارات الداخلية أو أجهزة الشرطة العربية لا تضم ضمن هيكلها التنظيمي إدارة أو قسم معني بحقوق الإنسان الرقمية، في حين أن (٢٩,٨٪) فقط من أجهزة الشرطة تتضمن مثل هذه الإدارات الحقوقية التي من شأن استحداثها أن يعزز احترام حقوق الإنسان الرقمية في العمل الأمني على نحو فعال من خلال الأدوار الوقائية والتوجيهية والرقابية التي يمكن أن تمارسها باستقلالية.

ثالثاً: الجانب القانوني والإجرائي المتصل بحقوق الإنسان الرقمية في العمل الشرطي:

السـؤال رقم (٣)	نعم	لا	غير متأكد	المتوسط الحسابي	الانحراف المعياري	معامل الاختلاف
هل تطبق مؤسستك قوانين جنائية أو تشريعات إدارية خاصة بالرقابة على حقوق الإنسان الرقمية؟	٥٨,٣	١٥,٥	٢٦,٢	٢,٤٣	٠,٧٤	٣٠,٦٦
السـؤال رقم (٨)	**نعم**	**لا**	**غير متأكد**	**المتوسط الحسابي**	**الانحراف المعياري**	**معامل الاختلاف**
هل تعتقد بوجود صعوبة في تحقيق التوازن بين متطلبات الأمن الوطني واحترام حقوق الإنسان الرقمية، كالحق في الخصوصية والحق في سرية البيانات الشخصية؟	٤٢,٩	٣٨,١	١٩,٠	٢,٠٥	٠,٩٠	٤٣,٨٨

يتضح من الردود الواردة على السؤال الثالث أن (٥٨,٣٪) من المشاركين أفادو بتطبيق مؤسساتهم لقوانين وتشريعات خاصة بحماية حقوق الإنسان الرقمية، بينما أنكر (١٥,٥٪) من المشاركين وجود مثل هذه التشريعات، بالإضافة إلى أن نسبة (٢٦,٢٪) غير متأكدين من وجود أو تطبيق قوانين جنائية أو تشريعات

إدارية خاصة في هذا المجال. ويبدو أن هناك لبساً في الفهم لدى من يظنون بتطبيق الشرطة لقوانين جنائية خاصة بحماية حقوق الإنسان الرقمية؛ إذ أوضح النقاش السابق أن الغالبية العظمى من الدول العربية لا تمتلك تشريعات معدة خصيصاً لحماية الحقوق الرقمية، وإن كانت تمتلك تشريعات عامة في مجال حقوق الإنسان ومكافحة جرائم المعلوماتية. كما تشير الردود على السؤال الثامن بأن (٤٢,٩٪) من المشاركين يعتقدون بوجود صعوبة في تحقيق التوازن بين متطلبات الأمن واحترام حقوق الإنسان الرقمية، وهو ما يدعو للقلق، ويدلل على بقاء الفكرة التقليدية الخاطئة التي تبرر مخالفة حقوق الإنسان من أجل الحفاظ على الأمن الوطني.

رابعاً: جانب بناء القدرات الشرطية الرقمية ذات العلاقة بحماية حقوق الإنسان الرقمية:

السـؤال رقم (٥)	نعم	لا	غير متأكد	المتوسط الحسابي	الانحراف المعياري	معامل الاختلاف
هل توفر المؤسسة أجهزة إلكترونية ذكية أو تطبيقات رقمية لأداء العمل الشرطي اليومي؟	٦١,٩	٢٣,٨	١٤,٣	٢,٣٨	٠,٨٤	٣٥,٤٤
السـؤال رقم (٦)	**نعم**	**لا**	**غير متأكد**	**المتوسط الحسابي**	**الانحراف المعياري**	**معامل الاختلاف**
هل تقدم المؤسسة خدمات إلكترونية حديثة للجمهور كتجديد الوثائق وتقديم البلاغات عبر الإنترنت؟	٧٢,٦	١٦,٧	١٠,٧	٢,٥٦	٠,٧٦	٢٩,٧٥
السـؤال رقم (٧)	**نعم**	**لا**	**غير متأكد**	**المتوسط الحسابي**	**الانحراف المعياري**	**معامل الاختلاف**
هل تتبنى مؤسستك استراتيجية أو خطة مستقبلية لبناء وتطوير القدرات الشرطية الرقمية؟	٧٣,٨	١٥,٥	١٠,٧	٢,٥٨	٠,٧٤	٢٨,٧٨
السـؤال رقم (٩)	**نعم**	**لا**	**غير متأكد**	**المتوسط الحسابي**	**الانحراف المعياري**	**معامل الاختلاف**
هل تعتقد بأن مؤسستك مواكبة للتطورات الرقمية بالمجتمع ومستعدة للتعامل معها؟	٦٤,٣	١٧,٩	١٧,٩	٢,٤٦	٠,٧٨	٣١,٥٩

يُلاحظ من الردود على الأسئلة الأربعة أعلاه حول بناء القدرات الشرطية الرقمية وجود مستويات جيدة من الجاهزية الرقمية؛ حيث بلغت نسبة الذين أكدوا توفير مؤسساتهم لأجهزة رقمية لأداء العمل الشرطي اليومي (٦١,٩٪)، وتقديم خدمات إلكترونية حديثة للجمهور (٧٢,٦٪)، وتبني المؤسسة لاستراتيجية شرطية لتطوير القدرات الرقمية (٧٣,٨٪)، لذلك يعتقد (٦٤,٣٪) من المستجيبين بأن مؤسساتهم الشرطية مواكبة للتطورات الرقمية ومستعدة للتعامل معها، مما يعكس انطباع عام بوجود اهتمام وتطور في هذا الجانب.

إلا أنه يُلاحظ من جانب آخر وجود تفاوت بين أجهزة الشرطة العربية في بناء القدرات الرقمية ذات العلاقة بحقوق الإنسان الرقمية، فضلاً عن بقية الجوانب المنوه عنها في الاستبيان، ومع التسليم بالظروف الاقتصادية لكل دولة، إلا أن الجهود الشرطية المنفردة والمزدوجة لا تخدم الأمن القومي المشترك للشعوب العربية، وبالتالي تظهر الحاجة لتبني استراتيجية عربية شاملة لمواجهة التحديات الرقمية المستقبلية وتعزيز التعاون الأمني العربي في مجال حقوق الإنسان، تحقيقاً لكرامة وسلامة وأمن الإنسان العربي في العصر الرقمي.

الخاتمة:

تناولت هذه الدراسة المتخصصة مسألة دقيقة وحساسة لم تحظ بالاهتمام اللازم في التشريعات والأبحاث الأمنية العربية؛ وهي مسألة حقوق الإنسان الرقمية في العمل الأمني، إذ بالرغم من الاهتمام الدولي المتصاعد بالتكنولوجيات الرقمية وما أفرزته من حقوق ومخاطر طالت كافة مجالات الحياة، ومنها المنظومة الأمنية في المجتمع، لا تزال المبادرات الشرطية العربية والجهود البحثية متواضعة في معالجة هذه المسألة الأمنية بالغة الأهمية، التي نالت نصيباً وافراً من العناية لدى أجهزة الشرطة الأجنبية دون العربية، بالرغم من عالمية الفضاء الرقمي وحتمية التحول الرقمي.

وقد ناقشت الدراسة في ثلاثة مباحث متسلسلة مفهوم حقوق الإنسان الرقمية ونطاقها، وبينت أبعادها الاجتماعية والاقتصادية والسياسية بالنسبة للمجتمع الدولي والدول العربية بصفة خاصة، وبناءً عليه، تم التأكيد على أهميـة إلمام الكوادر الشرطية العربية بحقوق الإنسان الرقمية أو حقوق الإنترنت، باعتبارها حقوقاً مستحدثة ذات قيمة عالية ربما تفوق في أهميتها حقوق الإنسان التقليدية في العصر الرقمي. وحددت الدراسة كذلك الانتهاكات الماسة بحقوق الإنسان الرقمية، سواء في جانبها المادي، أو الأخلاقي، أو تلك المخالفات التي تُنسب للأجهزة الأمنية، وتستدعي منها بالتالي يقظة وانتباه مضاعفين.

كما تناولت الدراسة دور أجهزة الشرطة في حماية وتعزيز حقوق الإنسان الرقمية، وذلك أولاً بمناقشة الأطر القانونية الدولية والوطنية المساندة لدور الشرطة في حماية الحقوق الرقمية، ثم باستعراض جهود ومبادرات أجهزة الشرطة الدولية والإقليمية في هذا المجال، وصولاً إلى تقييم جهود وتجارب أجهزة الشرطة العربية في حماية وتعزيز حقوق الإنسان الرقمية. وقد تم تعضيد الدراسة باستبيان لقياس وعي وجاهزية الكوادر الشرطية العربية للتعامل مع قضايا حقوق الإنسان الرقمية، حيث تم توزيعه على جميع أجهزة الشرطة العربية، وشارك فيه عدد مقدر من رجال الشرطة العرب، وبالإضافة إلى ما كشف عنه تحليل الاستبيان من نتائج وبيانات تم إدراجها في متن البحث، توصل البحث للنتائج والتوصيات التالية:

أولاً: النتائج:

- على غرار "حقوق الإنسان الأساسية" التي تلتزم الأجهزة الأمنية بحمايتها وتعزيز احترامها، تشير الصكوك الدولية إلى "حقوق الإنسان الرقمية" باعتبارها تشمل مجموعة واسعة من الحقوق الضرورية التي لا غنى للإنسان عنها في الفضاء الرقمي وعصر هيمنة خدمات الإنترنت.
- أظهرت الإحصائيات الإقليمية الصادرة في نهاية مارس ٢٠٢١ أن عدد سكان الوطن العربي بلغ ٤٢٣ مليون نسمة، وعدد مستخدمي الإنترنت وصل إلى ٣١٦ مليون، بزيادة ١,٩ مليون عن عام ٢٠٢٠،

حيث يشكلون ٧٤،٩٪ من عدد السكان، وبنسبة نمو بلغت ٥،٩٪ (internet world stats, 2021). بينما بلغ عدد مستخدمي الهواتف الذكية أكثر من ٢٠٠ مليون شخص، بنسبة ٥٠،٢٪ من عدد السكان، وبنسبة نمو عن عام ٢٠٢٠ بلغت ٩،٣٪. وتركزت أعلى نسبة لاستخدام الإنترنت في الفئة العمرية ما بين ١٥ و٢٤ عاماً، بنسبة ٦٧،٢٪ من عدد المستخدمين (ITU, Digital trends in the Arab States region, 2021).

- أكدت الإحصائيات الرسمية الصادرة في يناير ٢٠٢١ أن الدول العربية تتصدر المشهد الرقمي العالمي؛ حيث بلغ عدد مستخدمي الإنترنت في دولة الكويت٤،٢٦ مليون، بنسبة ٩٩٪، وبترتيب عالمي رقم (٦). وفي المملكة العربية السعودية بلغ عدد مستخدمي الإنترنت ٣٣،٥٨ مليون، بنسبة ٩٥،٧٪ من عدد السكان، وبترتيب عالمي رقم (٢٩). وفي جمهورية مصر العربية بلغ عدد مستخدمي الإنترنت ٥٩،١٩ مليون، بنسبة ٥٧،٣٪ من عدد السكان، لتحتل بذلك المرتبة (١٩) في الترتيب العالمي. وفي المملكة المغربية بلغ عدد مستخدمي الإنترنت ٢٧،٦٢ مليون، بنسبة ٧٤،٧٪ من عدد السكان، لتحتل المرتبة (٣٢) عالمياً. وفي المملكة الأردنية الهاشمية وصل عدد مستخدمي الإنترنت إلى ٦،٨٤ مليون، بنسبة ٦٦،٨٪ من عدد السكان، وبترتيب عالمي رقم (٣٨). كما لم تنخفض نسبة المستخدمين في بقية الدول العربية عن ٥٠٪ من عدد السكان (DIGITAL 2021).

- أدى الاعتماد المطرد ـ عالمياً وعربياً ـ على تكنولوجيا الاتصالات والمعلومات وخدمات الشبكة العالمية إلى تعاظم اهتمام الدول بالحقوق المرتبطة بها. ومن جانب آخر، نتج عن الارتفاع المتواصل في عدد مستخدمي الإنترنت، ارتفاع مقابل في الانتهاكات والاعتداءات الرقمية، كانت الساحة العربية مسرحاً للعديد منها، حيث تصدرت بعض الدول العربية القوائم العالمية في الاستهداف بأنواع الاعتداءات الرقمية والبرمجيات الخبيثة، في حين كانت بعضها أكثر مِنعةً وصموداً.

- بينما تتزايد أهمية حقوق الإنسان الرقمية في الحياة المعاصرة، وتتعاظم تبعاً لذلك المخاطر المحدقة بها، تبرز مسؤولية أجهزة الشرطة في حمايتها وتأمين ممارستها، إلا أن جهود أجهزة الشرطة العربية في هذا المجال الحيوي لا زالت في مراحلها الأولى، وبالمقارنة قطعت بعض أجهزة الشرطة الأجنبية أشواطاً كبيرة في ترسيخ احترام حقوق الإنسان الرقمية، بما يتوافق مع المعايير الدولية.

- بيَّنت الدراسة حجم الفجوة التشريعية في مجال حقوق الإنسان الرقمية بين الدول العربية ودول الاتحاد الأوربي التي أصدرت تشريعات وضوابط إجرائية متطورة في هذا المجال؛ أحدثها "ميثاق الحقوق الرقمية الأساسية للاتحاد الأوروبي".

- أشار تحليل استبيان قياس وعي وجاهزية الكوادر الشرطية العربية للتعامل مع قضايا حقوق الإنسان الرقمية إلى النتائج التالية:

- مما يقوض جهود ومساعي أجهزة الشرطة العربية في حماية وتعزيز حقوق الإنسان الرقمية؛ قلة وعي وإدراك الكوادر الشرطية بمعايير وضوابط التعامل مع هذه الحقوق، الأمر الذي قد يوقعهم في مخالفات قانونية.

- تعاني أجهزة الشرطة العربية من نقص في الأطر القانونية والتنظيمية المساندة، والتي ينبغي استكمالها من خلال إجراء مراجعة شاملة وتطوير التشريعات الجنائية والهياكل التنظيمية ذات العلاقة.
- على الرغم من التطور الملموس في القدرات الرقمية لأجهزة الشرطة العربية، إلا أن تبني تقنيات الشرطة الرقمية بما يواكب التحول المجتمعي الرقمي لا يزال متأخراً، مما قد يؤدي إلى تعميق الفجوة الرقمية بين المجتمع والشرطة، أو على الأقل بينها وبين الجماعات الإجرامية المنظمة.
- ومما يبعث على القلق، وجود اعتقاد بين بعض الكوادر الشرطية العربية بصعوبة تحقيق التوازن بين متطلبات الأمن الوطني واحترام حقوق الإنسان الرقمية.

- كما خلصت الدراسة إلى أن من أهم مواطن القصور التي تواجه الأجهزة الأمنية العربية هو غياب الاستراتيجيات والسياسات الرقمية بعيدة المدى، بالإضافة إلى عدم كفاية الهياكل المؤسسية، وضعف التعاون وتبادل الخبرات والتجارب حول تحديات حقوق الإنسان الرقمية في العمل الأمني.

- تأكدت أخيراً أهمية التعاون العربي الأمني في مجال حماية حقوق الإنسان الرقمية، من خلال تبادل المعلومات وعقد المؤتمرات والبرامج التدريبية المشتركة وورش العمل الإقليمية، وتأكدت كذلك أهمية مشاركة الدول العربية في الجهود العالمية وتعزيز التعاون والعمل المشترك مع المنظمات الدولية.

ثانياً: التوصيات:

- العمل وبأساليب علمية ومنهجية على رفع مستوى الوعي والثقافة المهنية لدى الكوادر الأمنية العربية بقضايا حقوق الإنسان الرقمية وحريات المجتمع الرقمي، مع التأكيد ـ وعبر دراسة حالات واقعية ـ على أن حماية حقوق الإنسان في العصر الرقمي لا توهِن بالضرورة الأمن الوطني، كما أن فاعلية الأداء الأمني تتحقق وتكتمل باحترام حقوق الإنسان.

- البُعد عن الأساليب التقليدية والنمطية في التدريب على حقوق الإنسان الرقمية ذات الطابع المتجدد، والتركيز على أساليب حديثة تقوم على الفاعلية والكفاءة وإمكانية مشاركة عدد غير محدود عن بُعد،

كدورات التعلم الإلكتروني الذاتية التي تتيح للمشاركين اختيار وقت التدريب والاطلاع على مقاطع تدريبية والتفاعل مع بعضهم وحضور ندوات متخصصة عبر الإنترنت.

- تبني مدونة عربية لقواعد سلوك الكوادر الأمنية في مجال حقوق الإنسان، وذلك أسوةً بمدونة الأمم المتحدة لقواعد سلوك الموظفين المكلفين بإنفاذ القوانين، بحيث تتضمن وبشكل واضح لا لبس فيه، المبادئ السلوكية والمعايير الأخلاقية التي يجب الالتزام بها عند إنفاذ القانون، بما يضمن احترام الحقوق والحريات العامة، ويُعزز مبدأ المساءلة في حال انتهاكها، صوناً لكرامة الوظيفة الأمنية، وتكريساً لمبدأ سيادة القانون.

- الاستمرار في دعم وتطوير إدارات حقوق الإنسان في وزارات الداخلية والأجهزة الأمنية العربية، وبذل الجهود لاستحداث إدارات مماثلة لحقوق الإنسان الرقمية في الدول الأخرى التي لم تخطو هذه الخطوة بعد، وذلك على نحو فعال يكفل استقلالها وقيامها بأدوارها التوجيهية والرقابية في هذا المجال.

- تحديث وتطوير الدساتير والتشريعات ذات العلاقة بحقوق الإنسان الرقمية، لمواكبة التطور التقني المتسارع والصكوك الدولية الحديثة ذات الصلة، مع مراعاة خصوصية المجتمعات العربية، وبما يخدم تطلعاتها للاستفادة من التكنولوجيات الرقمية الحالية والمستقبلية بشكل يعزز الثقة والأمان، مع عدم الاقتصار على إقرار عقوبات رادعة وإجراءات جنائية خاصة، وإنما أيضاً تنظيم أسواق تكنولوجيات المراقبة، وضمان التطبيق الفعال لهذه التشريعات.

- تنظيم عمل الأجهزة الأمنية العربية في مجال حقوق الإنسان الرقمية بمنظومة تشريعية شاملة ومتكاملة، توفر لها أساساً متيناً وواضحاً لتعزيز وحماية حقوق الإنسان، ومواجهة التحديات الناشئة عن العصر الرقمي، فضلاً عن تقنين إجراءات المساءلة القانونية في حال الإخلال بحقوق الإنسان، عبر فرض ضمانات إجرائية وضوابط رقابة وسبل انتصاف تضمن حماية الحقوق الرقمية في العمل الأمني على نحو فعال وشفاف.

- إيلاء المشاريع الشرطية للتحول الرقمي وبرامج رفع القدرات الرقمية للأجهزة الأمنية عناية خاصة، ويشمل ذلك التوسع في الخدمات الشرطية الرقمية المقدمة للجمهور، وتجهيز الكوادر الشرطية بأجهزة وتطبيقات رقمية لأداء المهام الأمنية، وتوظيف التقنيات الرقمية المتطورة لمكافحة الجرائم الرقمية المنظمة، وصولاً إلى تطبيق تقنيات الشرطة الرقمية بالكامل، وذلك ليس ترفاً، وإنما خدمة وطنية وضرورة عملية أدركتها الكثير من أجهزة الشرطة، لمواكبة العصر الرقمي وخدمة المجتمع الرقمي.

- إقامة شراكات وتعاون بين الأجهزة الأمنية والمراكز الوطنية لحقوق الإنسان ونقابات المحامين وغيرها من مؤسسات المجتمع المدني المعنية، وذلك لتعزيز الأمن المجتمعي، وتنفيذ بُنية أمنية جماعية فعالة لضمان احترام حقوق الإنسان، التي ليست مسؤولية الأجهزة الأمنية وحدها.
- دعم وتعزيز التعاون الدولي والتآزر الإقليمي في كافة مجالات حقوق الإنسان، واعتماد استراتيجية عربية أمنية موحدة لحماية حقوق الإنسان، تعكس وحدة مصالح الأمن القومي العربي الشامل.

المراجع باللغة العربية:

١. تقرير المنظمة العربية لحقوق الإنسان عن حالة حقوق الإنسان في الوطن العربي، القاهرة، ٢٠١٨.

٢. د. صونية عبديش، تحديات حماية الحق في الإعلام في البيئة الرقمية، مجلة دراسات في حقوق الإنسان، المجلد ٠٤، العدد ٠٢، ٢٠٢٠، ص ٨-١٨.

المراجع باللغة الإنجليزية:

1. Benedek, Wolfgang. 2019. *"International organizations & digital human Rights"* in Research Handbook on Human Rights & Digital Technology, Elgar.
2. Christou, G. 2016. *Cybersecurity in the European Union: Resilience & Adaptability in Governance Policy (New Security Challenges)*, Palgrave Macmillan.
3. EUISS. 2018. *Operational Guidance for the EU's international cooperation on cyber capacity building*, European Union.
4. HRC. 2016. Report on the Right to Privacy in the Digital Age UN Doc. A/HRC/27/37.
5. IMF. 2018. *Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment*, (WP/18/143).
6. INTERPOL Report Shows Alarming Rate of Cyberattacks during Covid-19, Interpol, 4 August 2020.
7. INTERPOL. 2020. ASEAN Cyberthreat Assessment: Key Insights from The ASEAN Cybercrime Operations Desk.
8. ITU. 2018. Global Cybersecurity Index (GCI) 2018.

9. ITU. 2020. Terms & Definitions. accessed 2021-3-10.
10. ITU. 2021. Digital trends in the Arab States region.
11. ITU. 2021. Guidelines for utilization of the Global Cybersecurity Agenda (GCA).
12. ITU-D Statistics. 2019. Measuring digital development: Facts and Figures.
13. Kaspersky Report, Jun 16,2020.
14. Kaspersky. 2020. Digital Dangerscape: Kaspersky Lab Spotlights Cybersecurity Trends in the Middle East, Turkey and Africa.
15. Kemp, S. 2020. *Global Digital Overview*. https://datareportal. accessed 2021-2-20.
16. Munich Security Report 2021, Between States of Matter Competition and Cooperation, Germany.
17. OECD, 2019. Global Cybersecurity Index 2019.
18. Office of the United Nations High Commissioner for Human Rights. 2004. Human Rights Standards and Practice for the Police, Geneva.
19. OSCE. 2016. Guide Book Representative on the Freedom of the Media.
20. Risk Based Security, 2019 year-end report: data breach Quick View, Virginia, 2019.
21. *Tele 2 Sverige AB v. Swedish Post & Telecom Authority*, judgment of 21 December 2016.
22. UN. Office of the High Commissioner for Human Rights (OHCHR). 2004. Human rights standards and practice for the police: expanded pocket book on human rights for the police, Geneva.
23. UN. 2020. Road map for digital cooperation, Geneva.
24. UNESCO. 2015. Keystones to Foster Inclusive Knowledge Societies: Access to Information and Knowledge, Freedom of Expression, Privacy and Ethics on a Global Internet, Final Study, Paris.

25. UNGA Resolution. 2010. Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructure, A/RES/64/211.
26. UNGA Resolution. 2018. The right to privacy in the digital age, A/RES/73/179.
27. UN Human Rights Council. 2020. Impact of New Technologies on The Promotion and Protection of Human Rights, Geneva, (A/HRC/44/24).
28. UN Human Rights Council. 2018. The Right to Privacy in The Digital Age, Geneva, (A/HRC/39/29).
29. UN Human Rights Council. 2018. Annual report on the right to privacy in the digital age, Geneva, (A/HRC/39/29).
30. WSIS, Tunis Agenda for the Information Society (2005), available at www.itu.int/net/wsis
31. Zalnieriute, Monika. 2019. *"Digital rights of LGBTI communities: a roadmap for a dual human rights framework"* in Research Handbook on Human Rights and Digital Technology, Elgar.

(ملحق)

استبيان قياس وعي وجاهزية الكوادر الشرطية العربية للتعامل مع قضايا حقوق الإنسان الرقمية

Questions Responses 84

Section 1 of 6

استبيان قياس وعي وجاهزية أجهزة الشرطية العربية للتعامل مع قضايا حقوق الإنسان الرقمية

Section 2 of 6

نبذة عامة:

يشارك الباحث (وهو أحد ضباط الشرطة بالدول العربية) في المسابقة البحثية للكوادر الشرطية التي ينظمها مجلس وزراء الداخلية العرب في مجال "حقوق الإنسان في العمل الأمني"، وذلك ببحث بعنوان "حقوق الإنسان الرقمية".

Section 3 of 6

أهداف الاستبيان:

1- قياس وعي الكوادر الشرطية العربية بقضايا حقوق الإنسان الرقمية في العمل الأمني.
2- تشجيع الكوادر الشرطية العربية على فهم حقوق الإنسان الرقمية واستيعاب تحديات العصر الرقمي.
3- استنباط الخبرات والتجارب الشرطية العربية في التعامل مع قضايا حقوق الإنسان الرقمية.
4- تقييم جاهزية أجهزة الشرطة العربية للتعامل مع متطلبات العصر الرقمي.
5- استخدام نتائج الاستبيان لتحديد سبل مواجهة التهديدات الرقمية وتعزيز حقوق الإنسان الرقمية.

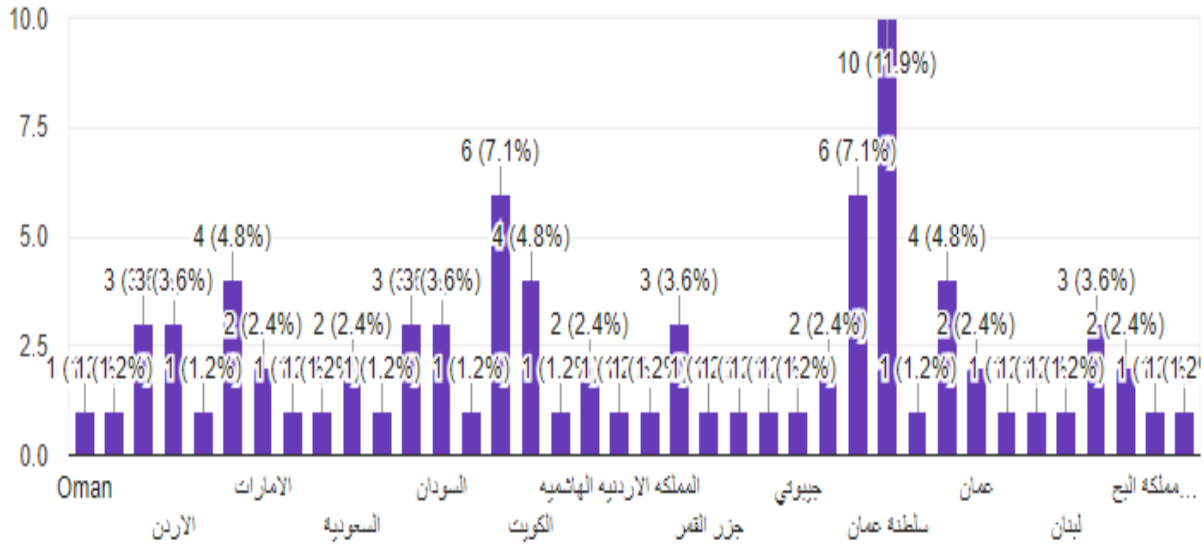
Section 4 of 6

المشاركون في الاستبيان:

منتسبي أجهزة الشرطة بالدول العربية

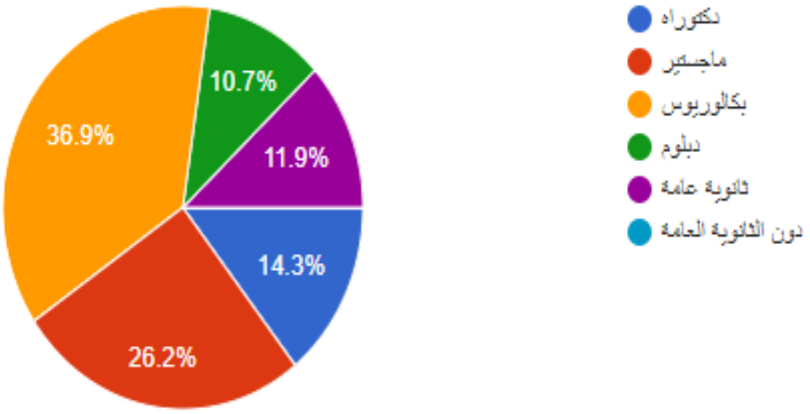
الدولة؟

84 responses



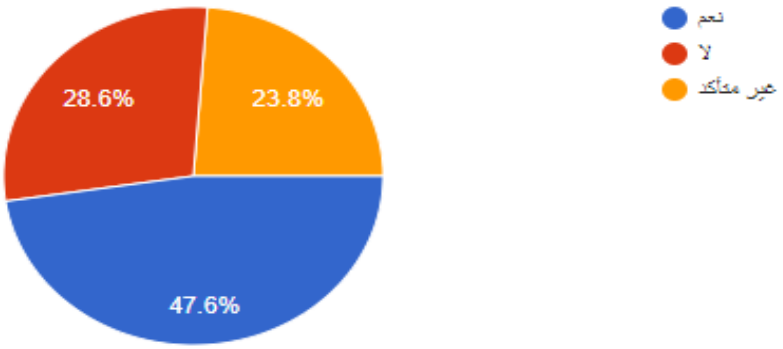
المؤهل العلمي؟

84 responses



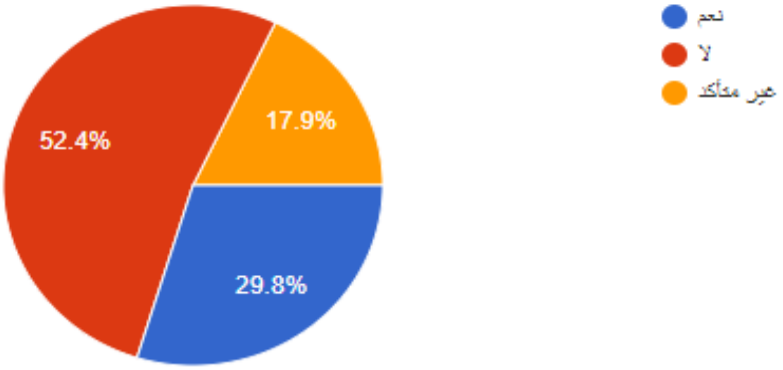
1- هل لديك إلمام ومعرفة بطبيعة وأنواع حقوق الإنسان الرقمية؟

84 responses



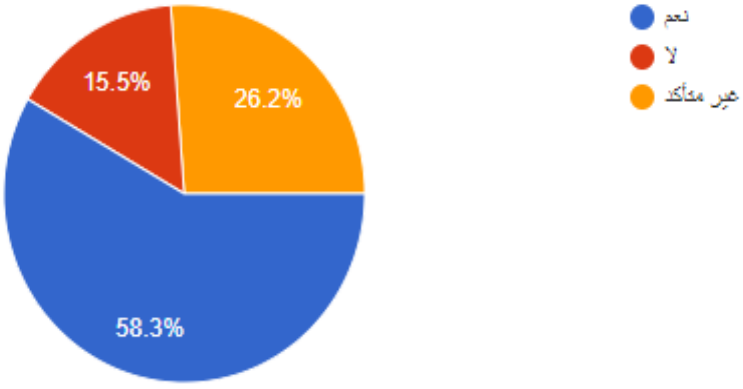
2- هل يوجد بالمؤسسة إدارة أو قسم مختص بحقوق الإنسان الرقمية؟

84 responses



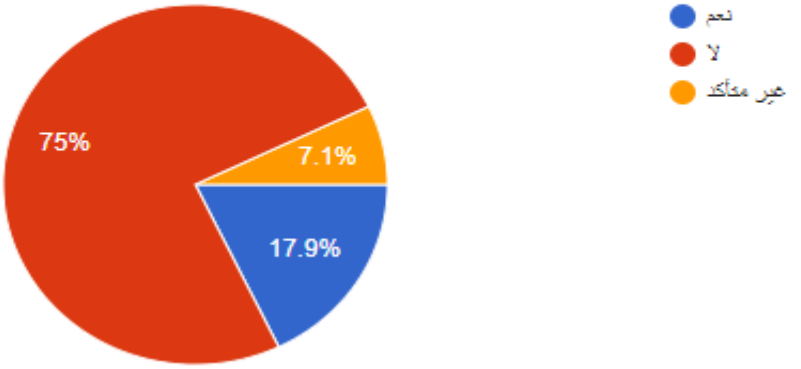
3- هل تطبق مؤسستك قوانين جنائية أو تشريعات إدارية خاصة بالرقابة على احترام حقوق الإنسان الرقمية؟

84 responses



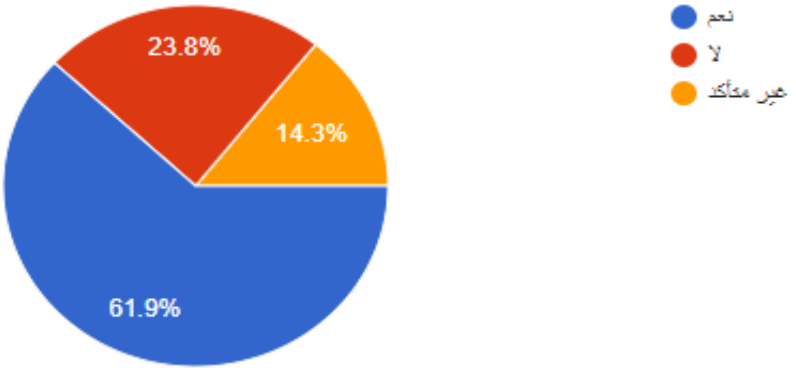
4- هل تلقيت تدريباً للتوعية بحقوق الإنسان الرقمية؟

84 responses



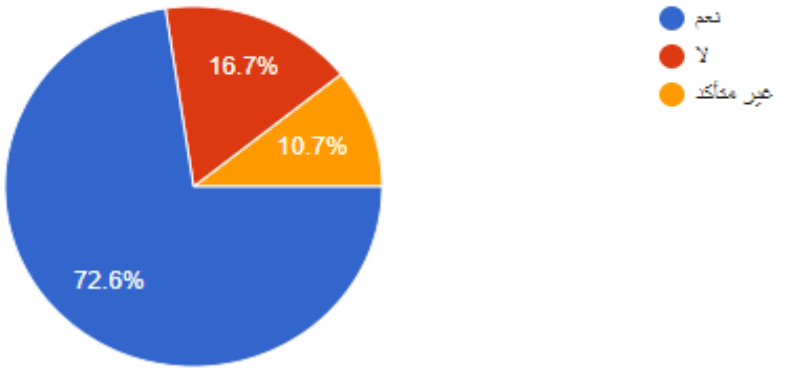
5- هل توفر المؤسسة أجهزة إلكترونية ذكية أو تطبيقات رقمية لأداء العمل الشرطي اليومي؟

84 responses



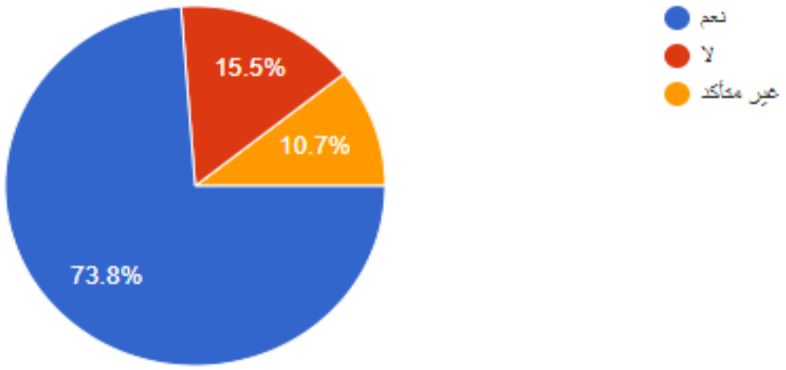
6- هل تقدم المؤسسة خدمات إلكترونية حديثة للجمهور كتجديد الوثائق وتقديم البلاغات عبر الإنترنت؟

84 responses



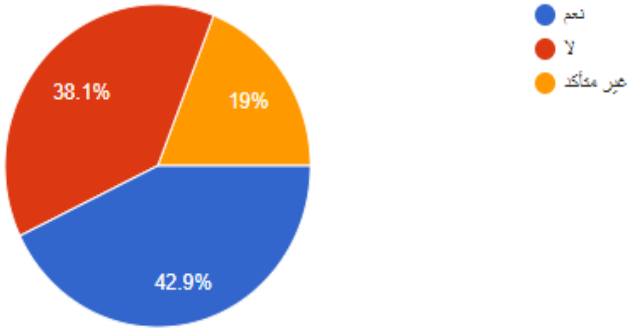
7- هل تتبنى مؤسستك استراتيجية أو خطة مستقبلية لبناء وتطوير القدرات الشرطية الرقمية؟

84 responses



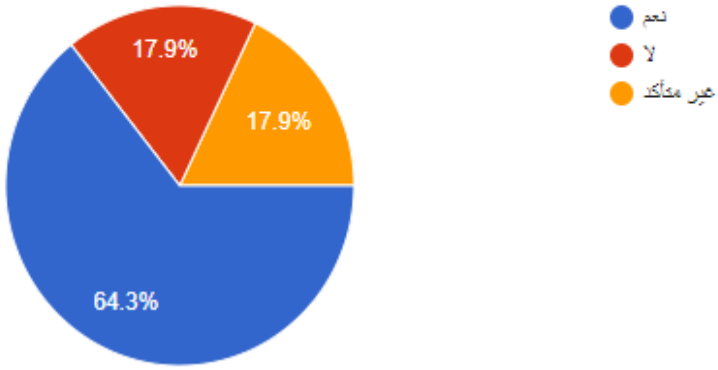
8- هل تعتقد بوجود صعوبة في تحقيق التوازن بين متطلبات الأمن الوطني واحترام حقوق الإنسان الرقمية، كالحق في الخصوصية والحق في سرية البيانات الشخصية؟

84 responses



9- هل تعتقد بأن مؤسستك مواكبة للتطورات الرقمية بالمجتمع ومستعدة للتعامل معها؟

84 responses



"تم بحمد الله وتوفيقه"