# التحديات الدستورية في مواجهة الجرائم المستحدثة

أ.م. د. عزيز سامي حسين
كلية الامام الكاظم (ع) للعلوم الاسلامية الجامعة

**كلمات مفتاحية:(الامن، السيبراني، الجريمة، الذكاء الاصطناعي، التزييف العميق)**

**المستخلص**
أصبحت الجرائم المستحدثة تشكل هاجس يؤرق الدولة والمجتمع على حد سواء فالدولة عليها مسؤولية حفظ الامن والنظام العام بكل ما ينطوي تحت هذين المصطلحين من تحديات، على ان الدولة وهي تمارس حقها في حفظ الامن والنظام العام ان تعمل على الموازنة بين انفاذ القانون والحقوق والحريات، وان لا يكون انفاذ القانون أداة للرقابة وقمع الحقوق والحريات التي كفلها الدستور، عندها تصبح دولة غير قانونية، وتتجاوز مبدا الشرعية الجنائية، وتمس بالحياة الخاصة، وهنا يثور سؤال يجب على الدولة مراعاته، اين يتم رسم الخط الفاصل في امن المجتمع وحقوق الافراد الدستورية.

اما مسؤولية الافراد فهي مسؤولية فهم القانون واستخدام حريته المكفولة دستوريا، وعدم التصرف بشكل يمكن ان يشكل انتهاك لحقوق وحريات اخرين، من خلال الامتناع عن الأنشطة التي تشكل جرائم مستحدثة مما تصبح ذريعة للسلطة العامة لتقليص الحريات تحت مبرر حماية النظام العام وحماية الأشخاص الاخرين من خلال توسيع صلاحيات المراقبة وبالتالي يمكن تصبح هذه الاعمال انتهاك بحقوق الافراد.

Abstract

Emerging crimes have become a growing concern that troubles both the state and society alike. The state bears the responsibility of maintaining security and public order, with all the challenges that these two concepts entail. However, while exercising its duty to preserve security and public order, the state must balance law enforcement with the protection of rights and freedoms. Law enforcement should not become a tool of surveillance or repression against the constitutional rights and freedoms guaranteed to individuals. Otherwise, the state risks losing its legal character, violating the principle of criminal legality, and infringing upon private life.

This raises an important question that the state must always consider: Where should the line be drawn between ensuring societal security and safeguarding constitutional individual rights?

As for individuals, they bear the responsibility of understanding the law and exercising their constitutionally guaranteed freedoms without infringing upon the rights and freedoms of others. They must refrain from engaging in activities that constitute emerging crimes, as such actions may provide the authorities with justification to restrict freedoms under the pretext of protecting public order and other persons. In turn, this expansion of surveillance powers could itself become a violation of individual rights.

**المقدمة**

شهد العالم خلال العقود الأخيرة تطورًا تقنيًا هائلًا في مجالات الاتصالات وتكنولوجيا المعلومات، مما أدى إلى بروز أنماط جديدة من الجرائم لم تكن مألوفة في السابق، أُطلق عليها اصطلاحًا "الجرائم المستحدثة". هذه الجرائم اتخذت طابعًا معقدًا وعابرًا للحدود، إذ لم تعد محصورة بإطار جغرافي أو زمني، بل استفادت من الانفتاح الرقمي والعولمة السيبرانية لتتسع وتتنوع في صورها وأساليب ارتكابها.

وفي ظل هذا التحول الرقمي السريع، برز الذكاء الاصطناعي كأحد أبرز أدوات العصر، بما يحمله من إمكانات هائلة في خدمة الإنسان، لكنه في الوقت ذاته

أصبح وسيلة يمكن توظيفها في تهديد الحقوق والحريات، لا سيما مع ظهور تقنيات مثل "التزييف العميق" Deepfake، التي تثير تحديات قانونية وأخلاقية غير مسبوقة تمس جوهر الخصوصية والحق في التعبير.

ولا يخفى أن العراق، كغيره من دول العالم، يواجه تحديات جدية في مجال الأمن السيبراني، نتيجة لضعف البنى التحتية، وغياب التشريعات المتخصصة، فضلًا عن الحاجة إلى استراتيجيات متكاملة لحماية الفضاء الرقمي الوطني من التهديدات المتزايدة. بناءً على ما تقدم، يهدف هذا البحث إلى دراسة الجرائم المستحدثة في سياقها المفاهيمي والقانوني، واستقصاء انعكاسات الذكاء الاصطناعي على الحقوق والحريات المكفولة دستوريًا، مع تحليل معمق للتحديات التي تواجه الأمن السيبراني في العراق، وبيان سبل مواجهتها وفق منظور قانوني شامل.

**أهمية البحث:**

تبرز أهمية هذا البحث في ضوء التطور المتسارع الذي يشهده مجال الذكاء الاصطناعي والتزييف العميق، والذي أصبح من أبرز سمات العصر الحديث. فقد اتسع نطاق استخدام هذه التقنيات ليشمل مختلف المجالات، سواء في الأوقات السلمية أو في حالات الصراع والحروب، مما يجعل دراسة هذا الموضوع ذات أهمية علمية وعملية.

**إشكالية البحث:**

أفرز التقدم التكنولوجي المتسارع في العصر الرقمي أنماطًا جديدة من الجرائم الإلكترونية المعقدة، اتسمت بطابعها العابر للحدود، وارتباطها المباشر بالتطورات في تقنيات الذكاء الاصطناعي، وعلى وجه الخصوص تقنية "التزييف العميق". وفي ظل غياب تشريعات وطنية متخصصة لمواجهة هذه الظواهر، أصبح الأمن السيبراني مهددًا على نحو متزايد، مما ينعكس سلبًا على حماية الحقوق والحريات الأساسية المكفولة دستوريًا.

ومن هنا تبرز الإشكالية الرئيسة لهذا البحث في التساؤل الآتي:

إلى أي مدى استطاع الإطار القانوني في العراق مواكبة التحولات الرقمية المستحدثة، بما يضمن حماية الأمن السيبراني وصون الحقوق والحريات في ظل تنامي استخدام تقنيات الذكاء الاصطناعي والجرائم المرتبطة بها؟

**نطاق الدراسة**

٥- سيكون نطاق بحثنا من حيث المكان النظام القانوني في العراق وهو أساس البحث مع الاستفادة من تجارب الدول الأخرى عربية او اجنبية وبقدر حاجة الدراسة

٦- من حيث الموضوع سيتم التركيز في هذا البحث على التحديات الدستورية في مواجهة الجرائم المستحدثة.

**منهجية البحث**

نظرًا لطبيعة موضوع البحث المتعلق بالجرائم المستحدثة وانعكاسات الذكاء الاصطناعي على الحقوق والحريات، تم اعتماد منهجية علمية تقوم على استخدام المنهج الوصفي التحليلي لتحليل مفهوم الجرائم المستحدثة وخصائصه، إلى جانب المنهج المقارن لمقارنة التشريعات الوطنية بالتشريعات الدولية. كما تم توظيف المنهج التحليلي النقدي لاستعراض أثر تقنيات الذكاء الاصطناعي والتزييف العميق على الحقوق والحريات، وتقييم مدى كفاية الأطر القانونية والأمنية القائمة في مواجهتها.

**هيكلية البحث:**

بغية الإحاطة بالدراسة ارتينا تقسيمه الى مطلبين نتناول بالمطلب الأول الإطار المفاهيمي للجرائم المستحدثة وبدوره سوف نقسمه الى فرعين الفرع تعريف الجرائم المستحدثة اما الفرع الثاني سوف نتطرق الى خصائص الجرائم المستحدثة وتميزها عن باقي الجرائم اما المطلب الثاني نخصصه للذكاء الاصطناعي والتزييف العميق انعكاساته على الحقوق والحريات وتحديات الأمن السيبراني في العراق وهو الاخر سوف نقسمه الى فرعين الفرع الأول انعكاسات تقنية التزييف العميق والذكاء الاصطناعي على الحقوق والحريات الدستورية والفرع الثاني التحديات التي تواجه الأمن السيبراني وفرص تحسينها في العراق ثم نختم الدراسة بأهم ما نتوصل اليه من استنتاجات ومقترحات .

**المطلب الأول : الإطار المفاهيمي للجرائم المستحدثة**

لحداثة هذه الجرائم في مجتمعنا المعاصر، وازديادها نوعا وكما، نتيجة التقدم العلمي والذي انصب بالخصوص على التطور الإلكتروني في مجال الإنترنيت والذكاء الاصطناعي وعالم الالكترونيات بشكل عام لذا وجدنا من الضرورة بيان الإطار المفاهيمي في الجرائم المستحدثة حيث ارتأينا في هذا المبحث من الدراسة بيان تعريف الجرائم المستحدثة من أجل الوقوف على المعنى الحقيقي لهذه الجرائم وهذا ما سوف نوضحه في الفرع الاول من هذا البحث كما ويكون من الضرورة بمكان بيان خصائص هذه الجرائم وهذا ما سنبينه في الفرع الثاني من موضوع هذا المبحث، وبغية الوصول إلى نتائج طيبة يقصدها رجال القانون رأينا من المفيد تمييز الجرائم المستحدثة عن الجرائم التقليدية وهذا ما سنبينه في الفرع الثالث من هذا المطلب.

**الفرع الأول: تعريف الجرائم المستحدثة**

يعد تعريف مفهوم الجرائم المستحدثة من الناحية الاصطلاحية ذا أهمية خاصة في إطار التحولات المتسارعة التي تطرأ على الواقع التقني والاجتماعي، لما لها من تأثير مباشر على تطور السياسة الجنائية واليات المواجهة القانونية. الامر الذي يحتاج الى دراسة تجمع بين الجانبين الفقهي والقانوني فالقوانين بالعادة لا تضع تعريفا محددا لهذا النوع من الجرائم وانما يترك الامر للفقه لتحديده ذلك لمرونة الظاهرة الاجرامية وتطور اشكالها

وكما رأينا أن التشريعات لم تتناول تعريف مصطلح الجرائم المستحدثة لذا نجد أن الفقه قد انبرى من أجل تعريف تلك الجرائم وبيان مفهومها إذ أن هناك من يعرف الجرائم المستحدثة بأنها: "جرائم قد تكون ذات جذور تقليدية ولكنها جرائم أخذت أشكالاً جديدة تتوافق مع التغيرات في البيئة الاجتماعية من وسائل تواصل وأساليب حياة جديدة تعتمد على الجوال والحاسوب والمعلومات والانترنيت... وغيرها، كما أنها قد تكون شكلا جديدا ناجماً عن البنى الاجتماعية والاقتصادية الجديدة المعلوماتية"[١] وايضا هناك من عرفها بأنها" أنماط من الجرائم التي لم يألفها المجتمع في السابق من حيث أسلوب ارتكابها ونوع من الجناة فيها وحجمها أو هي الجرائم المخطط لها التي يستعين المجرمون عند تنفيذها من معطيات العلم الحديث... أو هي التي يشترط لاستخدامها التقنية الحديثة لتسهيل تنفيذها واخفاء معالمها"[٢] وهناك من يرى بأنها

" أنماط من الجريمة تستخدم فيها التكنولوجيا الحديثة من أجل تسهيل عملية الأجرام مثل جرائم الإرهاب والجريمة المنظمة وجرائم العنف والجرائم الاقتصادية وأنماط الفساد الإداري وجرائم الحاسب الآلي وجرائم تزوير بطاقات الائتمان والجرائم الناتجة عن التعامل غير المشروع بجسد الإنسان وغيرها من أنماط الجرائم المستحدثة"[٣]

من خلال هذا التعاريف نجد أن الجريمة المنظمة تُعدّ أبرز صورة للجرائم المستحدثة. وذلك لأن أغلب صور الجرائم المستحدثة ترتكب بأساليب ووسائل حديثة من قبل نظام جماعة منظمة، تكون الجريمة المنظمة، وترتبط بالأشكال الجديدة للجريمة المنظمة عبر الوطنية، والتي اكدتها منظمة الأمم المتحدة في الاتفاقية العابرة للوطنية في العام ٢٠٠٠ التي تعد أساساً قانونياً محدوداً لمواجهة الأشكال المستحدثة للجريمة، كـ غسل الأموال، تهريب المخدرات، تهريب الأشخاص، الفساد، سرقة الأعمال الفنية، الإتجار بالأدوية المزيفة و .. غيرها .[٤]

كما أن الجريمة المنظمة عبر الوطنية هي إحدى صور الجريمة العالمية، حيث أن كافة أشكال الجرائم المكونة للجريمة المنظمة بأبعادها الجديدة هي من

طائفة الجرائم التي تستوجب التعاون في مجال مكافحة هذا النمط الاجرامي على المستويين الاقليمي والدولي.[١]

ومن ثم، يمكن وضع تعريف اوضح وأكثر شمولا لمفهوم الجرائم المستحدثة، بأنها:

هي الجرائم التي نشأت عن تطور الوسائل التقنية بالتالي تأخذ صورًا جديدة لم تكن معروفة من قبل، أو هي التي تُعيد صياغة الجرائم التقليدية في إطار حديث، بحيث يصبح من الصعب ضبطها بالوسائل التشريعية التقليدية، وهي في الغالب تمتد آثارها عبر الحدود الوطنية، مما يتطلب تعاونًا تشريعيًا وقضائيًا دوليًا لمواجهتها.

وعليه نحن نذهب مع من يستخدم اصطلاح الجرائم المستحدثة للدلالة على الجرائم المرتكبة بواسطة الوسائل التقنية الحديثة، والذي يشتمل على الجرائم القديمة بوجهها الحديث التي برزت على الساحة الإجرامية في عهدنا هذا، بالإضافة الى الجرائم التي لم تكن موجودة سابقاً وإنما ظهرت حديثاً وقد يظهر غيرها مستقبلاً بفعل التطور التقني، هذا من جهة، ومن جهة اخرى لأن هذا المصطلح ينطبق على الجرائم التي تتجاوز حدود الوطنية وتكون ذات طبيعة دولية، وتمس مصالح أكثر من دولة وبالتالي فإن مواجهتها تتطلب التعاون الدولي.[٢]

**الفرع الثاني: خصائص الجرائم المستحدثة وتميزها عن باقي الجرائم**

استكمالا لمعرفة الإطار المفاهيمي للجرائم المستحدثة لابد من التطرق الى اهم خصائص هذه الجرائم وهل لهذه الجرائم خصائص معينة تنفرد بها. لذلك سوف نتناول خصائص الجرائم المستحدثة ثم ننتقل الى ذاتية الجرائم المستحدثة.

**أولا: خصائص الجرائم المستحدثة**

للجرائم المستحدثة خصائص معينة تتمتع بها وهي: -

**١-الطبيعة العابرة للحدود**: واقع اليوم يشير إلى أن جزءاً كبيرًا من النشاط الإجرامي الخطير هو بطبيعته عابر للحدود الوطنية بطريقة أو بأخرى، اذ يرتكب هذا النشاط في دولة ما لتظهر اثاره في دولة اخرى أو ان يشارك فيها فاعلون من جنسيات متعددة هذه الخاصية جعلت تطبيق القانون الجنائي الوطني محدود الفاعلية الامر الذي يتطلب تدابير دولية للحصول على الأدلة أو تقديم المشتبه بهم إلى العدالة وفق اليات متعارف عليها مثل اتفاقية الامم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية ٢٠٠٠. كما ان نقل عائدات النشاط الإجرامي بطرق معقدة في جميع أنحاء العالم يعزز الحاجة الى تنسيق قانوني دولي. فهذه الظاهرة ليست محدودة في انتشارها الجغرافي. وبالتالي تعتبر من أهم الخصائص التي تعد ركيزة

في الجرائم المستحدثة، هي خاصية عبر الوطنية او الطبيعة العابرة للحدود، الامر الذي يتطلب استجابة إقليمية أو عالمية فريدة من نوعها لمكافحتها. وتخضع هذه الجرائم للقانون الجنائي عبر الوطني .[١]

٢-**جسامة الضرر**: الجرائم المستحدثة هي من اشد الجرائم خطورة ضررا على المجتمعات قياسا بالجرائم التقليدية، ويعود ذلك الى أسباب تتعلق بالوسيلة المستخدمة كونها وسيلة علمية متطورة وتتطور في كل لحظة نتيجة تطور المعرفة والعلم والتقدم التفني يضاف الى ذلك ان الجاني يمكن ان يرتكب الجريمة على بعد مسافات بعيدة عن مكان تواجده، فلا يتطلب الانتقال او التواجد في محل الجريمة وهذا بحد ذاته يسهل على الجاني ارتكاب الجريمة وفي ذات الوقت يصعب على الأجهزة المختصة الوصول اليه، هذه الأسباب وغيرها تجعل من هذه الجريمة ذا ضرر وخطر كبير .[٢]

-3**غياب التوافق الزماني والمكاني في الجرائم المستحدثة** : ان عدم اشتراط التوافق الزماني والمكاني بين الجاني والضحية او بين وقت ارتكاب الجريمة واكتشافها، تعد سمة أخرى من سمات الجرائم المستحدثة، بمعنى اخر قد تقع الجريمة في دولة معينة في حين تتجلى اثارها او يتضرر منها ضحايا في دولة اخرى حيث أن أهم مكون مميز للجرائم المستحدثة هو تدويل الجريمة وخروجها من الحدود الوطنية والإقليمية.

أن معظم الجرائم التقليدية تكون عادة ذات خصوصية اجتماعية من حيث الزمان والمكان، الا ان الجرائم المستحدثة تمارس في بنى اجتماعية مختلفة عن تلك البنى التي ظهرت فيها وارتبطت بها، كان هذا سببا الى تدويل هذه الجريمة، وأصبحت صورة الجريمة ذات طابع محلي اكتسب طابع دولي، هذا من جانب، اما الجانب الاخر فان هذه الجرائم يمكن ان تتفلت من العقاب بسبب غياب النظم القانونية او الفراغ التشريعي على المستوين المحلي والدولي، فالقانون الجنائي، والهيئات القائمة على تنفيذه، لا يزال يأخذ طابعاً إقليمياً مما يشكل في حد ذاته عاملاً وراء ظهور تلك الجرائم واستغلالها.[٣]

**ويترتب على هذه الخاصية تحديات قانونية منها:-**

١- صعوبة الاثبات: هذه الجرائم لا تترك اثار مادية واضحة الامر الذي يجعل اكتشافها واثباتها تحديا كبيرا مثال على ذلك جريمة اختراق انظمة الحاسوب قد تحدث دون عنف او تلف مادي الامر الذي يصعب معه ربط الفعل بالنتيجة وتحديد المسؤولية الجزائية .[٤]

٢- التدويل والبعد الاجتماعي: احد سمات الجرائم المستحدثة هي سمة التدويل ومرجع ذلك ان الجماعات الاجرامية المنظمة تخطط وتنفيذ

وهم لا يقيمون بالضرورة في دولة معينة وانما يمكن ان يقيموا في دول متعددة كون وسيلة الجريمة تتيح لهم التواصل وتبادل الأفكار وتحديد محل الجريمة والخطط الخاصة بالتنفيذ من خلال التواصل عبر التقنيات الالكترونية، لذلك اصبح العالم مدينة واحدة بواسطة هذه التقنيات العالية التطور، واصبح بالإمكان ان تكون الجريمة في دولة والمخطط لها في دولة أخرى والمنفذ من دولة ثالثة، وصور هذه الجرائم متعدد منها مثلا الاحتيال الكتروني او سرقة بطاقات الائتمان او غير ذلك من الجرائم .[١]

ج- ارتفاع **درجة التنسيق والتنظيم على الصعيد الدولي**: إن هذا النوع من الجرائم تتطلب بالضرورة درجة عالية من التنسيق والتنظيم، وهي بالغالب تعتمد على نظام سري معقد لا يمكن كشفها بسهولة الامر الذي يتطلب نظام اداري معقد فهي منظمات سرية تنتهج نظام اجتماعي معين، ولا تسمح بالكشف عن أعضائها ولها من الامكانية والنفوذ داخل مجتمعاتها، كما ان جرائمها تكون مخفية يصعب الكشف عنها لمل تملكه من إمكانيات تقنية عالية، إضافة الى البعد الجغرافي المميز لهذه الجرائم والذي يضفي صعوبة أخرى لكشف هذا النوع من الجرائم، ان هذه الجماعات هي جماعات منظمة عابرة للحدود كما بينت ذلك الأمم المتحدة في الاتفاقية الخاصة بمكافحة الجريمة المنظمة لعام ٢٠٠١.[٢]

**ثانيا: -تمييز الجرائم المستحدثة عن الجرائم التقليدية**

من أجل تقديم دراسة مستفيضة في موضوع بحثنا الموسوم التحديات الدستورية في مواجهة الجرائم المستحدثة فإنه يستحسن بيان أوجه التشابه والاختلاف بين الجريمة المستحدثة والجريمة التقليدية وهذا ما سنأتي في بيانه وفق الوجه الآتي:

**١: أوجه الاختلاف بين الجرائم المستحدثة والجرائم التقليدية**

لا يجوز الخلط بين مفهومي الجريمة التقليدية والجريمة المستحدثة، ذلك أن تحديد عناصر كلتا الجريمتين يتم على أساس القوانين الوطنية، ولا يؤدي بأي حال إلى التداخل فيما بينهما، لأن الجرائم المستحدثة غير مقتصرة على دولة بعينها، وإنما هي جريمة عبر وطنية. والأنشطة الإجرامية عبر الوطنية يمكن أن تشكل تهديداً مباشراً للسيادة للدولة لأن لديها القدرة على تقويض سلطة الحكومات وشرعيتها .[٣]

إن الجرائم المستحدثة أكثر تعقيداً مقارنة بالجرائم التقليدية، حتى ولو تعلق الأمر بجرائم من نوع معين، حيث تطور الطاقة الجرمية للفرد مع تطور الوسائل الجرمية المساعدة، وبالنتيجة أصبح نطاق الجريمة أكثر اتساعاً. ويرتبط ذلك

بالتوسع الهائل في التجارة العالمية والزيادة الهائلة في الهجرة، وتدويل أسواق العملات والانتقال السهل بين الدول والاتصالات الإلكترونية، وعلى الرغم من أن هذه الآثار المترتبة على العولمة قد أشاد بها الاقتصاديون، وفقهاء علم الإجرام، لكن يجب على واضعي السياسة الجنائية أن يتصدوا للفرص التي خلقتها العولمة، إلى جانب انفجار التكنولوجيات الجديدة، الذي ساعد على ظهور الجرائم عبر الوطنية أو الى تحول هذه الجرائم إلى أشكال أكثر خطورة .[١]

وعليه فإن مواجهة هذه الجرائم تصطدم على الصعيدين الموضوعي والإجرائي بصعوبات أكدها الواقع العملي في كثير من البلدان منه ما يتعلق بتطبيق نصوص التجريم التقليدية على الجرائم المستحدثة كون ان الوسيلة المستخدمة في الجريمة هي وسيلة تقنية أساسها فني علمي، هذا النمط الاجرامي المرتكب بهذه الوسيلة يمكن ان يكون عائق كبير بالكشف عن هذه الجريمة بسبب الخصائص الفريدة التي تتمتع بها، يضاف الى ذلك ان النصوص التجريم التقليدية لا تصلح مع هذا النوع من الجريمة لسبب ان هذه النصوص تتعامل مع وسيلة ذات طبيعة مادية فحين ان الجرائم المستحدثة وسيلتها ليست مادية وبالتالي تصبح هذه النصوص عاجزة امام هذه الجرائم.[٢]

كما ويمكن التمييز بين الجرائم التقليدية والمستحدثة من حيث إن الجرائم التقليدية جرائم محددة بنصوص قانونية لا جريمة إلا بنص وبالتالي لا عقوبة إلا بنص، وعليه متى ما مست هذه الجرائم مصالح يقررها القانون على انها مصلة محمية او خالفت سلوك مطلوب، وجب انزال العقوبة المستحقة والملائمة مع الفعل المرتكب.

اما الجرائم المستحدثة فهي جرائم عابرة للحدود الوطنية، ولم تتمكن التشريعات الوطنية من التصدي لجميع هذه الجرائم، ومنها على سبيل المثال الإرهاب الإلكتروني[٣]. حيث لا تتصدى لها التشريعات الوطنية إلا نادراً، أي بإدراج نصوص خاصة بها وتفتقر إلى التعريف التشريعي[٤]. ومرجع ذلك أسباب فنية تقنية متعلقة بتلك الجرائم وسرعة تطور هذه الجرائم، لكن ذلك لا يمنع واضع السياسة الجنائية من أن يتصدى لهذه الجرائم على المستوى الوطني لها من خلال اصدار التشريعات الداخلية لمكافحتها والنص عليه بشكل صريح. وبهذا الخصوص يلاحظ إن قانون منع إساءة استعمال أجهزة الاتصالات رقم ٦ لعام ٢٠٠٨ الصادر في إقليم كوردستان العراق عاقب كل شخص يمكن ان يستخدم جهاز الخلوي او أي جهاز اتصال اخر او استخدام الانترنيت او البريد الالكتروني بهدف الإساءة مثل القذف او السب او نشر اخبار يمكن تسبب الرعب.[٥]

اما ما يتعلق بالنص الخاص بنشر الأخبار المختلقة التي تثير الرعب باستخدام الوسائل المشار إليها كان من الممكن أن يؤخذ بعين الاعتبار في مواجهة الارهاب الإلكتروني في حالة القيام بذلك لدوافع إرهابية، وهو ما نص عليه قانون مكافحة الارهاب العراقي رقم ١٣ لعام ٢٠٠٥ وقانون مكافحة الإرهاب في إقليم كوردستان العراق. [١] هذا فضلاً عن الأسباب الموجبة لصدور قانون منع إساءة استعمال أجهزة الاتصالات التي جاءت بعيدة عن هدف مواجهة الارهاب عامة، والإرهاب الإلكتروني خاصة.

وكذلك من أبرز اوجه الاختلافات التي لا بد من التطرق إليها بين الجريمة التقليدية والجريمة المستحدثة المعلوماتية ان الأخيرة هي جريمة ناعمة، حيث لا وجود للعنف فيها على عكس الجرائم التقليدية مثل جريمة الإرهاب والسرقة والسطو المسلح وغيرها من الجرائم، اذ ان عملية نقل البيانات من جهاز حاسوب الى اخر أو السطو الإلكتروني على أرصدة بنك معين لا يستوجب من الجاني ان يستخدم العنف ولا يتبادل إطلاق النار مع رجال الأمن فاستخدام المعلومات هي المرتكز الاساسي لهذه الجريمة[٢]

**٢ : أوجه الشبه بين الجرائم المستحدثة والجرائم التقليدية:**

إن الجريمة المستحدثة تتفق مع الجريمة العادية أو التقليدية في كون كل منهما سلوكاً إجرامياً خارجاً عن القوانين والتشريعات الوطنية. وعليه يمكن توظيف تعريف الجريمة التقليدية لبيان مفهوم الجريمة المستحدثة مع إضافة أهم ما تتسم به الجريمة المستحدثة من خصائص. وقد تقترب الجرائم المستحدثة كثيراً من الجرائم التقليدية بوجه عام، وذلك لما لهما من أهمية وخطورة على الرغم من استقلال الجريمتين عن بعضهما البعض في بعض الخصائص والآثار الجسيمة المترتبة على الجرائم المستحدثة في ظل العولمة وافرازاتها السلبية.[٣]

يتبين مما سبق أن تمييز الجرائم المستحدثة عن التقليدية لم يعد مرتبطا بالشكل او النطاق فحسب، وانما يمس كذلك جوهر السياسة الجنائية. حيث كشفت هذه الجرائم قصور النظام التشريعي الوطني في التعامل مع السلوك الإجرامي الحديث، الامر الذي يستدعي تحديث اليات التجريم والعقاب والإجراءات القانونية لغرض مواكبة التقدم التقني العابر للحدود الوطنية وضمان حماية المجتمع بفعالية.

**المطلب الثاني: الذكاء الاصطناعي والتزييف العميق: انعكاساته على الحقوق والحريات وتحديات الأمن السيبراني في العراق.**

يتمتع التقدم التكنولوجي بأهمية بالغة في عالم الالكترونيات والإنترنيت والذكاء الاصطناعي نتيجة التطور الملحوظ في هذه المجالات في عصرنا الحديث، وخاصة في السنوات الاخيرة من هذا العصر الذي يشهد الصراع الكبير بين الدول العظمى "مثالها الويلات المتحدة الامريكية ودولة الصين الشعبية" في سبيل السيطرة على صناعتها والتقدم أكثر فأكثر، حيث نجد أن هناك صراع محتدم بين الدول العظمى من أجل السيطرة على المواد الأولية التي تدخل بهذه الصناعات والتطور في مجال الالكترونيات والذكاء الاصطناعي و دخول هذا التطور في كافة صعد الحياة، ان كانت صناعية او المجالات المختلفة الأخرى مثل استخدام الحروب التي سميت بالحرب السيبرانية، لذا وجدنا من المفيد تعريف الذكاء الاصطناعي "التزييف العميق" وانعكاساته على الحقوق والحريات الواردة في الدستور العراقي لعام ٢٠٠٥ وهذا ما سنتناوله في الفرع الأول ثم نبين في الفرع الثاني المعوقات والتحديات التي تواجه الأمن السيبراني في العراق وفق الآتي:

**الفرع الأول:- انعكاسات تقنية التزييف العميق والذكاء الاصطناعي على الحقوق والحريات الدستورية.**

سوف نقوم بتعريف التزييف العميق ومن ثم انعكاسات الذكاء الاصطناعي على الحقوق والحريات الواردة في دستور العراق لعام ٢٠٠٥ وهذا ما سنأتي على بيانه وفق الآتي:

**أولا: التعريف بالتزييف العميق.**

نظرًا لحداثة ظهور مفهوم "التزييف العميق"، وما يشهده من تطور مستمر، فإن التعريفات المتعلقة به لم تستقر بعد على صيغة نهائية، إذ تختلف دلالاته بحسب السياق التقني المستخدم. وبما أن هذا البحث يهدف إلى استجلاء المفاهيم القانونية للمصطلحات المتداولة في الأدبيات القانونية، فإنه من الضروري التوقف عند المعنى والمدلول القانوني لمصطلح "التزييف العميق". وعليه، فقد ارتأينا في هذا الموضع من البحث تناول التعريف القانوني لهذا المصطلح، بما ينسجم مع طبيعة الدراسة القانونية وأهدافها.

عرف التزييف العميق بتعريفات متعددة وكل تعريف يأتي بحسب وجهة النظر التي يتم النظر إليه منها إذ عرف بأنه " عبارة عن نسخة متطرفة ملفقة

وهمية من بيانات سمعية وبصرية تم التلاعب بها من خلال أحد تطبيقات الذكاء الاصطناعي المعدة لذلك" [١]

ومن خلال استجلاء التعريف المتقدم نجد أن هذا التعريف يركز على صفة التزييف العميق دون أن يركز على الذاتية الكامن في مضمون التزييف.

كذلك عرف" بأنه اصطناع مقاطع فيديو مزيفة لأشخاص ما يصعب وربما يستحيل أحيانا اكتشاف تكييفها كذلك صور وتسجيلات صوتية تلك الجرائم التي صنفت ضمن الأخطر في مجال الذكاء الاصطناعي".[٢]

في حين هناك تعريف آخر ضيق للتزييف العميق إذ عرف من خلاله بأنه " التزييف الناشئ عن طريق التقنيات التي يمكنها تركيب صور وجه للشخص المستهدف ليظهر في فيديو يفعل أو يقول اشياء يفعلها الشخص المصدر".[٣]

وهذا التعريف للتزييف العميق هو تعريف قاصر؛ لأنه يشمل فئة من التزييف العميق وهي فئة face swap اي استبدال وجه حقيقي بآخر مزيف حيث يركز هذا التعريف على آلية عمل مميزة للتزييف العميق ولكن الحقيقة هي أن التزييف العميق يعدّ شكلا من أشكال الوسائط المركبة التي يتم تغيير مضمونها الرقمي وعليه لن يقتصر الغرض منه على سبيل المثال استبدال شبيه الفرد بآخر إذ تمتلك تقنية التزييف العميق القدرة على التلاعب بالخصائص البشرية من خلال أساليب توليدية عميقة.[٤]

ولتلافي القصور الذي اعترى التعريف الضيق للتزييف العميق طرح بعض الفقه تعريفا أوسع للتزييف العميق بأنه "اصطناع المحتوى المركب من الذكاء الاصطناعي والذي يمكن أن يقع فيه مزامنة الشفاه في مقاطع الفيديو التي تم تعديلها وجعل حركات الفم متوافقة مع تسجيل الصوت، وهذا هو التعريف الأقرب إلى الواقع فمحتوى التزييف العميق يظهر على الأغلب بصيغة مقاطع فيدوية يتم الاستعانة ببرامج الذكاء الاصطناعي لتظهر وكأن الكلام صادر عنه وبشكل يطابق حركات الرأس والشفاه باستخدام تقنيات عديدة.[٥]

ويعتبر التزييف العميق من الوسائل العدائية التي يمكن ان تستخدم ضد شخصية معينة او جهة ما لغرض تشويه صورتها او الاساءة الى سمعتها حيث استعملت هذه التقنية في صنع مقاطع فديو إباحية مزيفة لعديد من المشاهير واستخدمت في احيان كثيرة لخلق اخبار كاذبة ومحاولة خداع القراء فتقنية التزييف العميق تمكن اي شخص يملك حاسوبا ومتصل بالأنترنيت من ان يصنع صورا او مقاطع فديو واقعية لأشخاص حقيقيين او غير حقيقين ويجعلهم يفعلون اشياء لم يرتكبونها من الاساس.[٦]

الامر الذي يجعلها اداة مثالية لارتكاب جرائم الابتزاز الالكتروني والتزييف العميق يشمل تزييف المحتوى المرئي كما ذكرنا سابقا والمحتوى الصوتي ومن الامثلة على جرائم التزييف الصوتي حيث نشرت مجلة فورس Forbes""[١] في وثيقة لها اشارت بها الى حادثة سرقة بنك دبي الاسلامي في الامارات عام ٢٠٢٠ بعملية معقدة حيث تلقى مدير البنك مكالمة صوتية من مدير اخر يعرفه وادعى المدير الاخر ان الشركة كانت على الوشك بالقيام بأجراء عملية استحواذ وتحتاج من البنك ان يسمح لها القيام ببعض التحويلات المالية التي يبغ قيمتها ٣٥ مليون دولار عن طريق اظهاره لمدير البنك رسائل بريد الكتروني من المحامي المختص والمسؤول عن الصفقة حيث كان كل شيء امرا طبيعيا و لا يوجد ما يدعو للشك فاكمل مدير البنك جميع التحويلات المالية ولم يكن لديه اي علم انه كان جزءا من عملية احتيال كبيرة استخدم فيها المحتالون تقنية التزييف العميق من لغرض تزييف صوت المدير.[٢]

ومن خلال ما تبين سابقا ان التزييف العميق يشكل انتهاكا للخصوصية الشخصية التي حماها دستور ٢٠٠٥ واعتبرها حقا دستوريا لا يمكن التجاوز عليها، هذا الحق ضمن الحقوق والحريات الأساسية. ولكل فرد الحق في حفظ خصوصيته ويعتبر شرط ضروري لحماية حقوق أخرى مثل الحق في الشرف والسمعة والكرامة والحرية الشخصية والدين والرأي ومعلومات وبيانات الشخص الخاصة به كل هذه تعتبر من الحقوق التي تدخل في خصوصية الانسان ولا يجوز مساسها أو التجاوز والاعتداء عليها تعد من الحقوق المرتبطة بالإنسان فهي حق عام ومطلق ينبغي احترامه فحق الخصوصية تندرج ضمن الحقوق غير المادية فالغاية منها صون المصالح المعنوية وحماية الجوهر الإنساني للفرد والتزييف العميق يؤدي الى تعريض الحياة الخاصة للأفراد للخطر من خلال عملية الانتقام الاباحي والابتزاز الالكتروني.[٣]

شهد العالم أخيرا توسعا وتطورا كبيرا في مجال شبكة الانترنيت ومنصات التواصل الاجتماعي على اختلاف تسمياتها واغراضها مما زادت معه تهديدات خصوصية الافراد واصبح معها لزاما استخدام وسائل تقنية ووضع تشريعات وإجراءات يمكن من خلالها الوصول الى الجناة مع الحفاظ على التوازن بين حقوق وحريات الافراد في خصوصيته وبين حق السلطة العامة في الحصول على الأدلة، ويجب ان تحاط هذه الأدلة المتحصلة بسرية ولا يمكن استخدامها الا من قبل الجهات التحقيقية والقضائية، حتى لا يمكن استخدامها او استغلالها من قبل جهات خارج هذه الأطر لأهداف شخصية وبالتالي تكون سبب لانتهاك الخصوصية.[٤]

وفي هذا المجال ونتيجة لهذا التطور التقني الذي فرض تحديات لم تكن موجودة سابقا اصبح واجب على المشرع العراقي احداث نظام قانوني جديد يواكب هذا التطور ويحافظ بدوره على الحقوق والحريات لجميع الأطراف كون الجرائم المستحدثة تختلف عن الجرائم ، فالأدلة تحتاج الى تحليل ودراسة من قبل مختصين وبالتالي لا يمكن قبولها مالم تكن على قدر كاف للإدانة ويمكن في هذا المجال استخدام الذكاء الاصطناعي او أي تقنيات أخرى في الدراسة والتحليل منها على سبيل المثال تقنيات تشفير الصوت الرقمي في الجرائم التي يكون معرفة الصوت كدليل اثبات في التحقيق الجنائي.[١]

**ثانيا :- الذكاء الاصطناعي وانعكاساته على الحقوق والحريات الدستورية**

تُعدّ الحقوق والحريات اهم الضمانات التي كفلها الدساتير للإنسان وكذلك القوانين والمواثيق الدولية والاعلان العالمي لحقوق الانسان والدستور العراقي لسنة ٢٠٠٥ اكد تلك الحقوق بما لا يتعارض مع ثوابت ومبادئ المجتمع وتقاليده الاصلية الملتصقة به، من اهم تلك الحقوق والحريات هي الحق في المساواة الحق في الامن الحق والحرية و العيش في ظروف بيئية سليمة، والحرية الشخصية هي حرية التعبير عن الرأي وحرية التفكير وحرية المعتقد وحرية التنقل والسفر.[٢]

لكن التطور السريع في التكنولوجيا وخاصة تطبيقات الذكاء الاصطناعي و ما يدخل الى البيت العراقي من انتهاك للخصوصية، و الحريات الخاصة بالتعبير والفكر والرأي و تزايد تطبيقات منصات التواصل الاجتماعي المختلفة له أهمية بالغة في ظل الاعداد المتزايدة التي تستخدم هذه التطبيقات و لساعات طويلة باليوم الواحد حيث أشارت وزارت الاتصالات العراقية في احدث إحصائية لها انها سجلت زيادة نسبة مستخدمي الانترنت في العراق ارتفاعا قياسيا بلغ نسبة٨٢,٩ بالمئة من السكان بنهاية عام ٢٠٢٤ بالمقارنة بعام ٢٠١٩ حيث كانت النسبة ٤٤,٣، بالمئة وذلك وفقاً للبيانات الرسمية الصادرة عن الاتحاد الدولي للاتصالات (ITU) .[٣]

ان هذه الشبكات المتنوعة والمختلفة في المضمون والاهداف تتيح للمستخدمين التواصل والتفاعل بدون قيود -عدا القيود التي تضعها الشبكة نفسها وهي عادة تكون لمصلحة الشبكة -وفي أي وقت وفي أي مكان من العالم كان لها الأثر الواسع في اتجاهين الاتجاه الإيجابي وهذا لا ينكر وليس في صدد الحديث عنه والجانب السلبي وهو محمور دراستنا حيث غير المفاهيم السائدة في المجتمعات لبعض مرتادي هذه المنصات مما شكل أفعالا تمس الحقوق والحريات الشخصية للأفراد وبنفس الوقت تشكل تحديا يواجه الدولة والمجتمع كونها لا

تتناسب مع تقاليد ومبادئ و دين المجتمع ومنها أيضا مواجهة اراء العنف والإرهاب وخطابات الكراهية والطائفية والشائعات المضللة وغيرها .

ان استخدام تطبيقات الذكاء الاصطناعي يبقى يثير قلقا واسعا بشأن اثر تلك التطبيقات على الافراد خاصة في مجال التعبير عن الرأي والحرية الشخصية حيث ان الدولة لهه العديد من المخاوف بشأن استخدام تقنيات الذكاء الاصطناعي في تنظيم المحتوى من حيث تمكين الجهة المختصة من حجب المحتوى غير اللائق و غير القانوني او على الأقل تقييده. في حين لا يمكن تقييد الاستهزاء والسخرية والتنمر على سبيل المثال وهذا ما أكدته محكمة العدل الدولية في قضية عرضت امامها على ان الأنظمة الآلية التي لا تميز بين المحتوى القانوني وغير القانوني هي انظمة فاشلة لأنها تنتقص من الحريات الخاصة بالأفراد.[١]

عليه تبقى مسؤولية الجهات المعنية بإزالة وحجب المحتوى غير القانوني مسؤولية تفرضها القوانين النافذة. كذلك مسؤوليتها في ملاحقة الجناة وتقديمهم الى الفضاء وما كشفت عنه وزارة الداخلية العراقية أخيرا من خلال الوصول والقبض على شخص يبلغ من العمر عاما ١٤قام بتحريض ٣٠ شخصا على الانتحار وتم الانتحار بناء على هذا التحريض من خلال لعبة تدعى روبلكس " Roblox Game" يذكر ان الأشخاص ليسوا عراقيين الا شخص واحد وهذا دليل على ان هذه الجرائم لا يحدها موقع جغرافي او حدود دولية.[٢]

وعلى إثر ذلك قامت وزارة الاتصالات العراقية بحضر اللعبة على مواقع التواصل الاجتماعي وأصدرت بيان بخصوص ذلك بينت به أسباب الحضر .[٣]

ان امر الحجب في القضية السابقة جاء بناء على الامر الولائي الصادر من المحكمة الاتحادية العليا والذي الزم بحجب المواقع الإباحية والمخلة بالآداب والمسيئة للأديان والمعتقدات والأشخاص ان قرار المحكمة جاء بناء على طلب من مقدم من احد أعضاء مجلس النواب العراقي وكان امر الحجب يشمل المواقع وشبكات الأنترنت والتوصل الاجتماعي وتطبيقات التواصل التي تتضمن صنعة ونشر المقاطع الجنسية والايماء والاغراءات الجنسية المخلة بالأخلاق والآداب العامة وتضمن القرار حجب المحتوى الخادش للحياء والتجاوز على الذات الإلهية وحرمة الكتب المقدسة وعلى الأنبياء والرسل والرموز الدينية والبغاء والشذوذ الجنسي والتعرض للأخرين والسخرية من الأديان والمذاهب، كما أشار القرار الى التزام وزارة الاتصالات وهيئة الإعلام بحجب الترويج والنشر للفسق والفجور وأشار القرار الى حجب مواقع تتضمن إساءة على ادأب وقيم المجتمع العراق.[٤]

ان هذه الأفعال التي إشارة اليها المحكمة الاتحادية وألزمت الجهات المختصة بحجبها وازالتها جميعها أفعال مجرمة بموجب قانون العقوبات العراقي وقوانين جنائية ساندة، كونها تعد اعتداء على الحقوق والحريات.

ان انتهاك الحريات الشخصية وحق التعبير عن الراي لا يقتصر على المواقع والمنصات وتطبيقات التواصل بل يتعدها الى تقنيات أخرى وهذا يرجع الى التطور السريع في تقنيات المعلوماتية والفضاء الرقمي وتطور وسائلها ومنها على سبيل المثال هو استخدام الكاميرات الذكية ذات القدرة العالية على تحليل الصور والمقاطع المتحركة من خلال تطبيقات وبرمجيات الذكاء الاصطناعي وما يمس ذلك من حياة الشخصية للأفراد بنشر الصورة خلال ثواني الى العالم حيث يستوجب توفر الامن القانوني للمعاملات المنجزة والمساندة من خلال المراقبة[١]

كما ان يمكن ان تعد هذه التقنيات وسيلة مضيقة لحق في حرية التعبير عن الراي عندما تستخدم التعرف على الوجوه اثناء التظاهر السلمي مثلا مما يؤثر على حرية الافراد في التعبير عن آراءهم ومترددين في الإفصاح عما يجول في خاطرهم إزاء ذلك التعرف وملاحقة السلطات لهم، حيث تمارس الحكومات ضغطا على الشركات الخاصة بمواقع التواصل الاجتماعي من اجل ان تكون على مقدرة من إزالة المحتويات تلك المحتويات التي تعتبرها الحكومات ضارة اليهم في حين تعتبر مسالة مهمة وتمثل حق من حقوق الافراد وهو حرية التعبير عن الراي والفكر فهذه الملاحقة تزيد من الانتهاكات على حقوق الانسان في هذا المجال.[٢]

ان مسالة التوازن بين مقتضيات الامن ومتطلبات الشرعية الدستورية هي مسالة غاية في التعقيد تتطلب التوفيق بين الحماية الجنائية والضمانات الدستورية فمن جانب ان الدستور اقر ضمانات أساسية تمثل حقوق وحريات الافراد وتمنع الاعتداء عليها ومن جانب اخر ان الافراد يعتقدون ان وضع قيود قانونية هي تحد من هذه الحقوق. لذا يتطلب عند استخدام الفضاء الرقمي والذكاء الاصطناعي يجب ان يكون هذا الاستخدام لا يمس حقوق وحريات الاخرين والا وجب تطبيق القانون ومنع الإساءة الى حقوق الاخرين

**الفرع الثاني: التحديات التي تواجه الأمن السيبراني وفرص تحسينها في العراق**

استكمالًا لمسار هذا البحث، وسعيًا لتقديم دراسة، وإن كانت بسيطة، تُسهم بشكل ما في تسليط الضوء على موضوع الأمن السيبراني، ارتئينا التطرق إلى التحديات التي تواجه الأمن السيبراني في العراق، وكذلك فرص تحسينه. وقد تمَّ تقسيم هذا المحور إلى فرعين رئيسيين: يتناول الفرع الأول أبرز التحديات التي

تعيق تحقيق أمن سيبراني فعّال في العراق، بينما يستعرض الفرع الثاني الفرص المتاحة لتعزيز وتطوير هذا المجال الحيوي. وسيتم توضيح ذلك تفصيلًا كالاتي:

**أولا: -أبرز التحديات التي تعيق تحقيق أمن سيبراني فعّال في العراق**

عرفت وزارة الداخلية العراقية مديرية الامن السبراني الأمن السيبراني على انه " مجموعة الإجراءات والتقنيات، والسياسات المستخدمة، لحماية الفضاء السيبراني، من التهديدات والاختراقات، والحد من الهجمات الإلكترونية.

وعرفت الفضاء السيبراني على انه " هو البيئة الافتراضية التي تتكون من أجهزة الكترونية متصلة بشبكة سلكية او لاسلكية، تحتوي على انظمة تشغيل وبرامج وتطبيقات وبيانات، وتمكن الأشخاص والمؤسسات من التواصل وتبادل المعلومات مع بعضها" والعراق يواجه تحديات هائلة نتيجة للتقدم التكنولوجي السريع والتحولات الكبيرة في مجال الاتصالات والمعلومات، فيعدّ هدفا استراتيجيا للهجمات السيبرانية لضعف الأمان الإلكتروني في البنية التحتية الوطنية، تلك التحديات تتفاقم بسبب استخدام المؤسسات العراقية لخدمات خارجية تتيح للمعلومات المهمة تداولها في خوادم خارج الحدود الوطنية، مما يفتح بابا لاختراقات واستخدامات غير مشروعة، مما ينتج عنها اعمال تجسسيه، أو حتى للمساس بأمان الدول الأخرى ويمكن أيجاز عددًا من تلك التحديات

**١ : ضعف البنية التحتية التكنولوجية:**

التطور التكنولوجي الذي شهده العراق في مجال الاتصالات والمعلومات والذي تزامن مع ضعف البنية الأمنية الإلكترونية التحتية الوطنية انتجت تهديدات الأمن السيبراني وهي تحديات غير مرئية" تؤثر على منظومة الأمن الوطني العراقي ، مع قلة الإمكانيات البشرية والفنية، أدى الى ان يكون العراق من الدول الضعيفة تقنيا امام الهجمات السيبرانية هذه من جانب من جانب اخر ان جميع الموسسات العراقية والشركات الخاصة تلجا الى مصادر خارجية في المسائل الالكترونية الخاصة في الفضاء الرقمي، وهذا عامل اخر يسبب عدم سيطرة الدولة على هذه الشبكات، وبالتالي اصبح ساحة هجوم سيبراني من الخارج على داخل العراق وهجوم سيبراني من الداخل الى الخارج.

عليه يجب تشكيل مجموعة من الاطر القانونية والتنظيمية والهياكل التنظيمية والتقنية والتكنلوجية حيث تمثل جهود مشتركة للقطاع العام والخاص، وذلك لحماية الفضاء السيبراني العراقي والتركيز على ضمان توافر أنظمة للمعلومات وحماية سرية للمعلومات وحماية الخصوصية واتخاذ جميع الاجراءات اللازمة لحماية المواطن من مخاطر الفضاء السيبراني.

وحسب استراتيجية الامن السيبراني في وزارة الداخلية العراقية حيث جعلت من مديرية الأمن السيبراني مديرية أمنـية معلوماتـية ولها مهام حماية

الأمــن السيبراني وتعمل على ارساء وتعزيز جهود هذه الوزارة من خلال بناء منظومــة فعالــة للأمــن الســيبراني وبهدف تطوير وتنظيم عملها بشكل يؤمن ويحافظ على الامن الوطني للمؤسسات وكذلك الحفاظ على امن الافراد وعلى خصوصيتهم من خلال منع او الحد من تلك التهديدات.[١]

ورغم هذه الجهود لكن غياب الوسائل والتقنيات الحديثة وقلة الخبرة في هذا المجال مقارنة ما تملكه المجموعات متطرفة وهاكرز غير معروفين، يشهد العراق بين الحين والآخر هجمات سيبرانية قبل البنية التحتية الحكومية والقطاع الخاص، مما يؤثر سلبا على الخدمات الحكومية ويعرض الأفراد والمؤسسات لمخاطر جرائم الاحتيال وسرقة الهوية؛ لذلك فإن ضعف الأمان السيبراني يؤثر على استقرار العراق.[٢]

**٢ : ضعف تشريعات الأمن السيبراني:**

أن استخدام التقنيات المستحدثة للتحكم في المعلومات واساليب تجميعها ومعالجتها واختزانها وتحسين الانتفاع منها من خلال الحاسبات وثورة الاتصالات، والسرعة والتطور التكنولوجي في العراق والعالم، مع وجود فجوات قانونية في مجال الإنترنت تشكل تحديًا كبيرًا ، ففي ظل غياب معايير موحدة لقوانين الإنترنت، يصبح التنظيم أمرًا حيويًا، خاصة عندما تتعلق المسألة بأفراد أو كيانات من دول مختلفة ويظهر الخلل بشكل واضح عندما يتورط الهجوم السيبراني في قضايا تجاوز الحدود؛ إذ قد يقوم المهاجمون بتنفيذ هجمات إرهابية في بلد لا تكون فيه قوانين صارمة، مما يثير تحديات في مجال تنازع القوانين، وتكمن المشكلة الحقيقية في عدم وجود سلطة مركزية على مستوى دولي تعمل على تطبيق قوانين تحمي الخصوصية وتضمن الأمان الرقمي.

يصبح الحل لهذه التحديات هو التعاون الدولي الفعال، وفي ظل غياب سلطة دولية مركزية، يزيد نشوء ظاهرة الإرهاب الإلكتروني فهي التحديات التي تواجه الأمان الوطني.

ان حماية الخصوصية وضمان الأمان السيبراني، يجب وضع معايير وسياسات تنظيمية دولية تحدد التزامات يجب اتباعها في البيئة السيبرانية، وتعمل على توحيد الجهود التعاون الدولية هذه ستكون أساسية لتحقيق أمان الإنترنت ومواجهة التهديدات السيبرانية بفعالية .[٣]

ان عدم وجود تشريعات محددة في العراق لمكافحة الهجمات السيبرانية يتيح للمهاجمين والهاكرز فرصة لتنفيذ أنشطتهم دون مواجهة عواقب قانونية جادة، يمكن أن يؤدي هذا الوضع إلى عجز في تحقيق العدالة وتطبيق القانون على

المخترقين مما يزيد من التهديدات ويقلل من فعالية الاستجابة لتحسين الأمان السيبراني في العراق.

**٣ : غياب الأمن الالكتروني:**

بينا سابقا وفي عدة مواضع من هذه الدراسة حجم المخاطر المحدقة بالعراق نتيجة التطور المتسارع والهائل في مجال الفضاء الرقمي وتكنلوجيا الانترنيت مع زيادة وحجم الاستخدام الذي اصبح واقعا لا يمكن الاستغناء عنه، يرافقه تهديد امني سيبراني ان كانت من داخل الدولة او خارجها.

ونتيجة ضعف البنية الأساسية وعدم مواكبة تطورات الامن السيبراني وخاصة ان العرق بقى بعيدا عن هذه التكنلوجيا فترات طويلة من الزمن. وبعد التغيير في العام ٢٠٠٣ اقتحمت هذه التكنلوجيا بشكل كبير كل المرافق الحيوية العراقية وعلى حد سواء في القطاعات العامة والخاصة، ونتيجة لتطور الجريمة مع هذا التطور، وعلى أهميتها الإيجابية ، الا ان الواقع يشير الى جوانب سلبية كبيرة وكبيرة جدا في ظل غياب تشريعات وطنية وكذلك الاتفاقيات الثنائية او الإقليمية او الدولية الفعالة خاصة وان هذه الجرائم جرائم عابرة للحدود مثل جرائم النصب والاحتيال والاستغلال والجرائم المالية، وكذلك الاستخدام السلبي لمواقع التواصل الاجتماعي للوصول بإعمال مدمرة.

**ثانيا: -البناء الاستراتيجي للأمن السيبراني في العراق**

تسعى الحكومة العراقية إلى تحسين أنشطتها وخدماتها من خلال تبني التقنيات الرقمية، وعكس نموذج تحليل نضوج الحكومة الرقمية، ومدى تكامل هذه التقنيات في أنظمة الحكومة، ويعرض هذا السياق تحديات تبني التحول الرقمي والفرص المتاحة، ويسلط الضوء على استراتيجيات العراق في تطوير حكومة رقمية تعزز التقدم والفعالية في إطار نظمها السياسية وبذلك تبنت الحكومة العراقية استراتيجيات شاملة بعد العام ٢٠٠٣ يمكن الإشارة اليها بإيجاز:

١- استراتيجية الامن القومي للعام ٢٠٧ وجاءت من خلال وثيقة الامن القومي وتهدف الى( حماية شبكات الاتصالات، وأنظمة المعلومات، والدفاع ضد الهجمات المعلوماتية، وتامين الحكومة الالكترونية) كما اشارت الوثيقة الى بناء هياكل الانترنت في العراق، وتنظيم استخدامه المجال الالكتروني.[١]

٢- استراتيجية الامن السبراني ٢٠١٧ كانت اكثر وضوحا من سابقتها من حيث البناء الاستراتيجي فيما يخص الامن السيبراني من حيث الخطوات العملية والتنفيذية والمديات الزمنية فضلا عن مستويات التنفيذ والتشريع والقضاء، كذلك تحديدها لأشكال ومصادر التهديد

السيبراني، وبناء منظومة امن سيبرانية وإتاحة وسائل تنفيذية اكثر فعالية لتحقيق الامن السيبراني، وتحديد فترة زمنية قصيرة ومحددة لذلك. مع عدم اغفال الجانب الثقافي والمعرفي المجتمعي للأمن السيبراني.[١]

٣- اما استراتيجية الامن القومي للعام ٢٠٢٥ -٢٠٣٠ فقد وضعت تعريف للأمن السيبرني ضمن الملحق رقم(١) عندما عرفت المفاهيم لاستراتيجية الامن الوطني العراقي وكيفية حماية مؤسسات الدولة والافراد من الهجمات السيبرانية والتهديدات التي تؤثر على امن المعلومات وخصوصية الافراد [٢]

٤- كما ان الحكومة بدورها سعت بدورها لبناء هياكل لحماية الامن السيبراني ومنها أ٠ مديرية الامن السيبرني التابع لوزارة الداخلية والذي سبق وان تم ذكره في مواضع سابقة من هذا البحث وحددت مهام وصلاحيات هذه المديرية من خلال وضع السياسات والاستراتيجيات الخاصة بالأمن السيبراني ومتابعة تنفيذها [٣]

ب٠ مديرية الامن السيبراني في وزارة الدفاع والتي انشات في العام ٢٠٢٢ ويهدف الى حماية الفضاء السيبراني للوزارة ذاتها

ج٠ جهاز الامن الوطني هدفه جمع المعلومات وتحليل التهديدات والمشاركة الفعالة ضد مختلف الأنشطة التي تهدد الامن السيبراني

د٠ مركز البيانات الوطني في الأمانة العامة لمجلس الوزراء ويهدف على الاشراف على البوابة الحكومية الموحدة للخدمات الالكترونية

ه٠ فريق الاستجابة لحوادث الامن السيبراني وهو فريق امني متخصص بمجال الامن السيبراني والاستجابة للحوادث السيبرانية وحماية البنية التحتية للأنترنت تم انشاه من قبل مستشارية الامن الوطني في العام ٢٠١٧

و٠ جهاز المخابرات الوطني وهذا الجهاز من الأجهزة الحساسة والمهمة في العراق ولا يعرف الكثير عنه نظرا لحساسيته ويتمتع بإمكانية كبيرة في مجال الامن السيبراني والتهديدات التي تواجه العراق.

وفي مجال الخبرة والتدريب ومن خلال التنسيق مع حلف الناتو تم تدريب ١٦ موظفا من فريق الاستجابة في مجال اساسيات الدفاع السيبراني وحماية البيانات من التسرب وكذلك جمع الأدلة الالكترونية وتحليل الشفرات.[٤]

**الخاتمة**

بعد الافراغ من كتابة هذه الدراسة وصلنا الى اهم الاستنتاجات والمقترحات

**الاستنتاجات:**

١. كشفت الدراسة عن وجود مجموعة من التحديات التي تواجه الأمن السيبراني في العراق، منها ضعف البنية التحتية التكنولوجية، وغياب تشريعات فعّالة في مجال الأمن السيبراني، فضلاً عن نقص الإجراءات الأمنية الإلكترونية الفعالة.
٢. خلصت الدراسة إلى أن الجرائم المستحدثة تختلف عن الجرائم التقليدية في عدة جوانب، رغم وجود بعض أوجه التشابه، ما يميزها بجملة من السمات المستقلة التي تستوجب معالجات قانونية خاصة.
٣. توصلت الدراسة إلى أن للذكاء الاصطناعي تأثيرًا مباشرًا على عدد من الحقوق والحريات المكفولة بموجب دستور جمهورية العراق لسنة ٢٠٠٥، لا سيما حرية الرأي والتعبير، وحرية الفكر، والحرية الشخصية
٤. أشارت النتائج إلى وجود فرص حقيقية لتحسين الأمن السيبراني في العراق، من خلال حماية البنية التحتية للمعلومات الحيوية، وتطوير آليات الاستجابة للحوادث والهجمات الإلكترونية، بالإضافة إلى تعزيز ثقافة الأمن السيبراني وزيادة الوعي بالمخاطر السيبرانية.

**المقترحات:**

١- ضرورة التفات المشرع بإقرار القوانين اللازمة التي تنظم وتعالج الجرائم التي تحصل بواسطة التطور الحاصل في الذكاء الاصطناعي والتزييف العميق.
٢- نقترح على الجهات ذات العلاقة والتي تكون مسؤولة بضرورة العمل على إنشاء وتطوير مرافق تهتم بالذكاء الاصطناعي كون أن العمل في هذا المجال والعمل على تطويره أصبح ضرورة ملحة في أغلب دول العالم حيث إن السباق محتدم وكبير في هذا المجال لما له من أهمية بالغة وكبيرة على كافة الصعد والمجالات.
٣- التزام الدولة بالعمل بتأهيل وتدريب الكوادر القضائية والأمنية المتخصصة للتعامل مع هذه الجرائم المعقدة والتحديات التقنية والقانونية.
٤- ضرورة مراعاة المشرع عند وضعه نص تجريمي ان يكون هذا النص ذو صياغة قانونية واضحة ومحددة للجرائم المستحدثة بما يكفل الحقوق الدستورية لمنع التفسيرات الواسعة التي تنتهك مبدا الشرعية الدستورية.

**الهوامش**

١. نقلا عن عبد الكريم الردايدة، الجرائم المستحدثة واستراتيجية مواجهتها، دار الحامد للنشر والتوزيع، عمان، ط١، ٢٠١٣، ص ١٥.

٢. محمد الأمين البشيري، التحقيق في الجرائم المستحدثة، اكاديمية نايف للعلوم الأمنية، الرياض، ٢٠٠٤، ص ٨-٩.

٣. عبد الله بن العزيز باليوسف، أساليب تطوير البرامج والمناهج التدريبية لمواجهة الجرائم المستحدثة، جامعة للعلوم الأمنية، الرياض، ط١، ٢٠٠٤، ص ٣٧.

٤. [1] - محمود محمد عبد النبي محمد، منهج التجريم في اتفاقية الأمم المتحدة للجريمة المنظمة عبر الوطنية، الموقع الالكتروني. https://search.mandumah.com/Record/455083 تاريخ الزيارة ٢٠٢٥/٤/١

٥. [1] - عادل يوسف عبد النبي الشكري، الجريمة المعلوماتية وأزمة الشرعية الجزائية، مجلة مركز دراسات الكوفة، ٢٠٠٨، العدد ٧، ص ١٢٢.

٦. [1] - في هذا المجال يسميها الجرائم المستحدثة انظر في هذا الشأن، هلالة محمد تقي محمد أمين، التعاون الدولي في مواجهة الجرائم المستحدثة، مكتبة يادكار لطباعة ونشر الكتب القانونية، السليمانية، ط١، ٢٠٢٠، ص ٢١.

٧. [1] نقلًا عن عبد الكريم الردايدة ، مصدر سابق ، ص ٦٤.

٨. [1] - جمال توفيق احمد، اهم الجرائم المستجدة والمستحدثة وآليات مواجهتها، مجلة العلوم والرياضة، المجلد الثاني، العدد الأول ، ٢٠١٩، ص ١٥.

٩. [1] - عبد الكريم الردايدة، مصدر سابق، ص ٦٥.

١٠. [1] عادل يوسف عبد النبي الشكري، مصدر سابق، ص ١٦.

١١. [1] -ممدوح عبد الحميد عبد المطلب، التنبؤ الأمني في عصر العولمة، ط١، جامعة نايف العربية للعلوم الأمنية، الرياض، دار الحامد والأكاديميون، الأردن، ٢٠١٤، ص١٨.

١٢. [1] - وثيقة الأمم المتحدة رقم A\CONF ٨١٢٢٢ . ، جدول الاعمال المؤقت وشروحه، مؤتمر الأمم المتحدة الثالث عشر لمنع الجريمة والعدالة الجنائية ، الدوحة ، ١٢-١٩ نيسان ٢٠١٥، ص١٥.

١٣. [1] - نقلًا عن هلالة، مصدر سابق، ص٢٣.

١٤. [1] - محمد احمد عليوي، التجريم الوقائي في الجرائم المستحدثة (رسالة ماجستير، معهد العلمين للدراسات العليا، ٢٠٢٠، ص ٣١.

١٥. [1] - عبد العال الدريبي، ومحمد صادق، الجرائم الالكترونية دراسة قانونية قضائية مقارنة مع احدث التشريعات العربية في مجال مكافحة الجرائم المعلوماتية والانترنيت، المركز القومي للإصدارات القانونية، القاهرة، ط١، ٢٠١٢، ص ١٢.

١٦. [1] ا- ايمن عبد الحفيظ عبد الحميد سلمان، الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية ، دار المطبوعات الجامعية الجديدة ، الإسكندرية، ٢٠٠٥، ص ٢٦.

١٧. ينظر: مشروع مكافحة جرائم المعلوماتية في التشريع العراقي لعام ٢٠١٢ متاح على الموقع الالكتروني http;\\www.slideshare.net\hamzoz\arabic-version-law وقانون منع اساءة استعمال اجهزة الاتصالات الكردستاني رقم ٦ لسنة ٢٠٠٨، وقائع كردستان العدد ٨٧ بتاريخ ١٧/ ٢٠٠٨/٦.

١٨. [1] - المادة ٢ من قانون منع إساءة استعمال أجهزة الاتصال الكردستاني رقم ٦ لسنة ٢٠٠٨. والتي نصت " يعاقب "... كل من أساء استعمال الهاتف الخلوي أو أية أجهزة اتصال سلكية أو لاسلكية أو الانترنيت أو البريد الالكتروني ذلك عن طريق التهديد أو القذف أو السب أو نشر أخبار مختلقة تثير الرعب ..."

١٩. [1] - المادة ١ من قانون مكافحة الإرهاب العراقي رقم ١٣ لعام ٢٠٠٥، الوقائع العراقية العدد٤٠٠٩ في ٢٠٠٥/١١/١٩.

٢٠. [1] - حسين عباس حميد، جريمة الابتزاز الالكتروني، مجلة القانون والدراسات والبحوث القانونية، كلية القانون جامعة ذي قار، العدد٢٢ ص٥٩٢.

٢١. [1] - د. هلالة محمد تقي محمد امين، مصدر سابق، ٢٥.

٢٢. [1] - نقلا عن: محمود سلامة عبد المنعم الشريف، جريمة الانتقام الاباحي عبر تقنية التزييف العميق Deepfake والمسؤولية الجنائية عنها ، جامعة الاسكندرية، ص ٣٦٩ .

٢٣. [1] - نقلا عن: محمود سلامة عبد المنعم الشريف، ص ٣٦٧.

٢٤. [1] - صدام فيصل كوكز المحمدي، - التزييف العميق- تقنيات معقدة واشكاليات قانونية - دراسة تحليلية قانونية مقارنة ، هاترك للطباعة والنشر والتوزيع ، العراق، أربيل ، ص ٨.

٢٥. [1] - اشرف سيد أبو العلا، المواجهة الجنائية، تقنية الديبفاك ، كلية الحقوق ، جامعة أسيوط، ص ٤٨٦.

٢٦. [1] - نقلا عن : صدام كوكز المحمدي، ص ٩.

٢٧. [1] - رضا ابراهيم عبد الله بيومي، الحماية القانونية من مخاطر تطبيقات التزييف العميق في الفقه الاسلامي والقانون الوضعي، دراسة تحليلية مقارنه، مجلة روح القوانين - كلية الحقوق جامعة طنطا عدد خاص - المؤتمر العلمي الدولي الثامن - التكنولوجيا والقانون

٢٨. [1] - فوربس(Forbes) هي شركة من شركات النشر والاعلام في الولايات المتحدة الامريكية

٢٩. [1] -انظر موقع جزيرة نت موقع ويب اخباري تابع لقناة الجزيرة على الرابط تاريخ https://www.aljazeera.net

٣٠. [1] - انظر الباب الثاني من دستور العراقي ٢٠٠٥، باب الحقوق والحريات.

٣١. [1] - اشرف سيد ابو العلا، المواجهة الجنائية لمخاطر تقنية الديب فيك، مجلة العلوم القانونية والاقتصادية، مجلد ٦٦، العدد٣، مؤتمر كلية الحقوق بجامعة عين شمس المنعقد في ٥ نوفمبر٢٠٢٣ حول التحديات والافاق القانونية والاقتصادية للذكاء الاصطناعي، ص٣٨.

٣٢. [1] - حسين المولى، حجية التسجيلات في الاثبات الجنائي، مقال منشور على الموقع الالكتروني

٣٣. https://www.bayancenter.org /٢٠٢٤/١١/١٢٦١٤/ تاريخ الزيارة ٢٠٢٥/٤/٢١.

٣٤. [1] - انظر المواد من (١٤ ولغاية ٤٦) من الدستور العراقي لسنة ٢٠٠٥.

٣٥. [1] - اعلام وزارة الاتصالات بتاريخ ١٢/ ٧ / ٢٠٢٥ الموقع الرسمي لوزارة الاتصالات العراقية على الموقع الالكتروني https://www.moc.gov.iq/?article=1053 تاريخ الزيارة ١١/ ١١/ ٢٠٢٥.

٣٦. [1] - case c-70/10 scarlet extended ECLI:EU:C:2011:771 para 52 :case c-٥٠360/10 SABAM ECLI:EU:C:2012:85<para ، الموقع الالكتروني، تاريخ الزيارة ١١/11/2025 https://curia.europa.eu/juris/liste.jsf?language=en&num=c-70/10

٣٧. [1] - قناة عربي BBC NEWS ، على الموقع الالكتروني: https://www.bbc.com/arabic/articles/czdrrpz6mvmo تاريخ الزيارة: ١١/١١/٢٠٢٥م.

٣٨. [1] - بيان لوزارة الاتصالات، أنه "حرصاً على حماية الأمن المجتمعي وصون القيم الأخلاقية والتربوية للأسرة والأطفال والحفاظ على سلامة مستخدمي خدمات الإنترنت في العراق، نعلن حظر لعبة "روبلوكس" داخل البلاد استناداً الى قرارات المحكمة الاتحادية العليا"، مضيفة أن "القرار يأتي بعد درس مستفيض ورصد ميداني أظهر أن اللعبة تتضمن عدداً من الأخطار الأمنية والاجتماعية والسلوكية، ومن بينها إتاحة التواصل المباشر بين المستخدمين بشكل يعرّض فئة الأطفال والمراهقين إلى محاولات استغلال أو ابتزاز إلكتروني، واحتواء اللعبة على مشاهد وسلوكيات تتنافى مع القيم والتقاليد المجتمعية"، مبينة أن "هناك إيحاءات جنسية وعمليات ابتزاز، فضلاً عن ألفاظ نابية وتجاوزات على الذات الإلهية وغيرها من السلبيات" اعلام وزارة الاتصالات العراقية بتاريخ ١٩ تشرين الأول ٢٠٢٥ الموقع الرسمي للوزارة https://moc.gov.iq/?article=1105 تاريخ الزيارة ١١/ ١١/ ٢٠٢٠.

٣٩. [1] - انظر الامر الولائي للمحكمة الاتحادية العليا المرقم ٣٢٥/ اتحادية / امر ولائي/ ٢٠٢٣.

٤٠. [1] - سحر عبد الستار إمام، انعكاسات العصر الرقمي على قيم وتقاليد القضاء، بحث منشور بالمجلة المصرية للدراسات القانونية والاقتصادية، العدد العاشر، مصر، يناير ٢٠١٨، ص ٢٠٠.

٤١. [1] - المصدر السابق نفسه ، ص ٢٠١.

٤٢. [1] - الموقع الرسمي وزارة الداخلية مديرية الأمن السيبراني متاح على الموقع الالكتروني https://moi.gov.iq/?article تاريخ الزيارة ١٢/ ١١/ ٢٠٢٥.

٤٣. [1] - رعد خضير صليبي ، تعزيز الامن السيبراني في العراق، جامعة بغداد، مركز الدراسات الاستراتيجية والدولية، قسم السياسة العامة، مجلة دراسات دولية، العدد ٩٩، ٢٠٢٤، ٥١٧.

٤٤. علي إبراهيم المعموري، الامن السيبراني وأثره في الامن الوطني العراقي بعد العام ٢٠٠٣، رسالة ماجستير، كلية العلوم السياسية، جامعة بغداد، ٢٠١٩، ٧٤-٧٥.

٤٥. [1] - انظر وثيقة استراتيجية الامن القومي (٢٠٠٧-٢٠١٠) مستشارية الامن القومي، بغداد، ص ٢٣. والتي تضمنت

أولا:" انشاء نظام توفير معلومات دقيقة وإيصالها بالوقت الصحيح لإسناد المصالح الوطنية قام النظام السابق ولعقود بعزل العراق وشعب العراق عن أغلب دول العالم، وكان هذا جلياً وواضحاً في مجال تقنية

المعلومات والإنترنت. ولغرض التخلص من هذه التركة الثقيلة، قررت الحكومة العراقية تبني – وبأسرع وقت ممكن – أكثر أنظمة تقنية المعلومات كفاءةً لغرض استخدامها في القطاعين العام والخاص. ومن خلال هذه الوسيلة تأمل الحكومة العراقية إكمال ربط العراق ومواطنيه بالمجتمع المدني. تتطلب الديمقراطية والإدارة الرشيدة إيصال معلومات دقيقة وكاملة في الوقت المناسب للمواطنين والمنظمات الخاصة ودوائر الحكومة، وهو أيضاً مهم لاستعادة الأمن والازدهار في العراق. ستقوم الحكومة العراقية الفيدرالية والدوائر التابعة لها والمؤسسات الأمنية بإنشاء أنظمة معلومات وأنظمة إدارة معلومات لزيادة الكفاءة والفعالية في تحقيق المهام

ثانياً. إدارة عمليات معلوماتية للتأثير على الجمهور المتلقي. إن العمليات المعلوماتية هي عنصر مكمّل لسعي الحكومة للتأثير على المجاميع المؤيدة والمضادة. يعتبر المجال المعلوماتي في الاستراتيجية الحديثة وفن الحرب موازياً للمجالات الدبلوماسية والاقتصادية والعسكرية. ولذلك فإن حكومة العراق والقوات الأمنية ستقوم بعمليات معلوماتية للتأثير على أنظمة المعلومات المعادية. في نفس الوقت تدافع عن أنظمة معلوماتها تجاه الهجمات المضادة. ستبذل الحكومة العراقية جهوداً خاصة لمنع نشر وتداول المعلومات الخاطئة والأعمال الدعائية التي كانت رائجة في زمن النظام السابق.

ثالثاً. إنشاء برنامج الحكومة الالكترونية لإسناد المصالح الوطنية: قررت حكومة العراق التقدم للأمام في عملية ربط المواطنين بالحكومة وشعب العراق بالمجتمع الدولي، وتعتبر تقنية المعلومات أحد أهم الأمور المساعدة في مد هذه الجهود. سيركز العراق بأقصى حد ممكن على التقنية اللاسلكية لتقليص الحاجة إلى استنزاف الوقت وإعادة إنشاء الشبكات الأرضية المكلفة. إن البرنامج الرئيسي لتنفيذ هذا الجهد هو مبادرة الحكومة الإلكترونية. تهدف الحكومة الإلكترونية لربط المواطنين بالدوائر الحكومية المسؤولة عن توفير الخدمات الأساسية لغرض تسهيل العمل بين الحكومة والمواطنين. إن الغرض من إنشاء الحكومة الإلكترونية هو للاستجابة السريعة لاحتياجات المواطنين بأقل وقت ممكن وتجاوز الاعمال الروتينية وبالاستفادة القصوى من معلومات الانترنت"

٤٦. انظر وثيقة استراتيجية الامن الوطني لعام ٢٠١٧ ،

٤٧. [١] - انظر وثيقة استراتيجية الامن الوطني لعام ٢٠٢٥-٢٠٣ حيث عرفت الامن السيبراني على انه "مجموعة من السياسات والإجراءات والتقنيات التي تهدف إلى حماية الأنظمة والشبكات الرقمية والمعلومات الالكترونية من الهجمات والتهديدات التي قد تؤثر على أمن المعلومات وخصوصية الأفراد والمؤسسات. يشمل هذا المجال حماية البيانات من السرقة أو التلاعب أو الإتلاف وضمان سلامة واستمرارية عمل البنية التحتية الرقمية، ويتضمن الأمن السيبراني عدة جوانب رئيسية، منها (حماية البيانات والمعلومات: لضمان سرية البيانات وحمايتها من الوصول غير المصرح به، وحماية الشبكات الإلكترونية من الهجمات التي قد تستهدف نقل البيانات عبر الإنترنت أو الشبكات المحلية، وضمان عدم تسرب أو تعطيل المعلومات).

٤٨. - [١] مهام مديرية الامن السيبراني هي ١- وضع السياسات والاستراتيجيات الخاصة بالأمن السيبراني ومتابعة تنفيذها.٢. ادارة الحوادث المتعلقة بالأمن السيبراني .٣. متابعة وكشف الثغرات الأمنية في المواقع الالكترونية الكشف عن الثغرات.٤. دراسة وسد النقاط الرخوة في البنى التحتية للشبكات السلكية واللاسلكية.٥. تحليل مواقع الانترنت ومواقع التواصل الاجتماعي.٦. تثقيف ونشر الوعي الامني بين منسوبي قوى الامن الداخلي وباقي شرائح المجتمع.٧. مراقبة وتحليل مراكز البيانات والمحطات الطرفية الخاصة.٨.الاستجابة والحد من عمليات اساءة استخدام تكنولوجيا المعلومات والاتصالات".

٤٩. مصطفى إبراهيم سلمان الشمري ، الامن السيبراني وأثره في الأمن الوطني العراقي، مجلة العلوم القانونية والسياسية، كلية القانون والعلوم السياسية، جامعة ديالى، المجلد ١٠، العدد ١، ٢٠٢١، ص ١٥٢.