ISSN: 2519 – 6138 (Print)
E-ISSN: 2663 – 8983(On Line)

TUJR
مجلة جامعة تكريت للحقوق
Tikrit University Journal for Rights

IRAQI Academic Scientific Journals
العراقية المجلات الاكاديمية العلمية

Tikrit University Journal for Rights
Journal Homepage : http://tujr.tu.edu.iq/index.php/t

كلية القانون
College of Law

Mechanisms for combating cybercrime at the national level and the administration's role in achieving it

Assistant Professor .Dr. Fawwaz Khalaf Dhahir

College of Law, Tikrit University, Salahaddin, Iraq
fawazkhalaf19@yahoo.com

Researcher. Emad Jasim Mohammed

College of Law, Tikrit University, Salahaddin, Iraq
emadjasim2019@gmail.com

Article info.

Article history:
- Received 1 September 2022
- Accepted 9 October 2022
-Available online 1 September2024

Keywords:
- Management
- crimes
- Combat
- informative
- mechanisms.

Abstract: Information crimes are cross-border crimes, which have begun to witness a wide spread in recent times, as a result of the scientific and technical development that the world has witnessed and is witnessing in a growing and accelerating manner, especially in the field of information technology, and the use of Internet means, which has become a wide space for communication between societies, in addition to what The world witnessed the emergence of the Corona pandemic and its attendant repercussions, at various levels, and the serious repercussions on the economies of countries, and the resorting of countries to the means of the Internet to run public facilities in them, and this matter was reflected on the crime scene, through the emergence and growth of information crimes, which began to spread and took space In the form that has begun to worry the

international community, and governments at the internal level, and that combating this type of crime requires the establishment of states through their national legislation, and the measures taken by the administration in order to combat these crimes, or at least reduce them, so it can The administration may undertake this task by following a set of verses to carry out this task in the optimal manner, and in a manner that achieves a kind of balance between the rights and freedoms of individuals in the issue of privacy and personal freedom. The personality they enjoy, guaranteed by covenants, international instruments, constitutions and national legislation, and the reduction of the commission of such crimes.

آليات مكافحة الجرائم المعلوماتية على المستوى الوطني ودور الإدارة في تحقيقه

أ.م.د. فواز خلف ظاهر

كلية القانون، جامعة تكريت، صلاح الدين، العراق
fawazkhalaf19@yahoo.com

الباحث. عماد جاسم محمد

كلية القانون، جامعة تكريت، صلاح الدين، العراق
emadjasim2019@gmail.com

معلومات البحث :

تواريخ البحث:
- الاستلام : ١/ ايلول/ ٢٠٢٢
- القبول : ٩ / تشرين الاول/ ٢٠٢٢
- النشر المباشر : ١/ ايلول/٢٠٢٤

الكلمات المفتاحية :
- إدارة
- جرائم
- مكافحة
- معلوماتية
- آليات.

الخلاصة: تعد الجرائم المعلوماتية من الجرائم العابرة للحدود، والتي بدأت تشهد انتشاراً واسعاً في الآونة الأخيرة، نتيجة التطور العلمي والتقني الذي شهده ويشهد العالم بشكل متنامي ومتسارع، وخاصة في مجال تقنية المعلومات، واستخدام وسائل الأنترنت، والتي بات فضاءً رحباً للتواصل بين المجتمعات، علاوة على ما شهده العالم من ظهور جائحة كورونا وما صاحبها من تداعيات، على مختلف الصعد، والانعكاسات الخطيرة على اقتصاديات الدول، ولجوء الدول إلى وسائل الأنترنت لتسيير المرافق العامة فيها، وهذا الأمر انعكس على مسرح الجريمة، من خلال ظهور وتنامي الجرائم المعلوماتية، التي بدأت بالانتشار وأخذت حيزاً كبيراً، بالشكل الذي بدأ يؤرق المجتمع الدولي، والحكومات على الصعيد الداخلي، وأن مكافحة هذا النوع من الجرائم يتطلب قيام الدول عن طريق تشريعاتها الوطنية، وما تقوم به الإدارة من إجراءات في سبيل مكافحة تلك الجرائم، أو الحد منها على أقل تقدير، لذلك فإنه يمكن للإدارة أن تضطلع بتلك المهمة باتباع مجموعة من الآيات للقيام بتلك المهمة على الوجه الأمثل، وبالشكل الذي يحقق نوعاً من التوازن بين حقوق وحريات الأفراد في مسألة الخصوصية والحرية الشخصية التي يتمتعون بها، والتي كفلتها العهود والصكوك الدولية، والدساتير والتشريعات الوطنية، وبين الحد من ارتكاب تلك الجرائم.

المقدمة : تعد الجرائم المعلوماتية من بين الجرائم العابرة للحدود، كونها لا تقتصر على دولة بعينها، أو نطاق جغرافي محدد، بسبب طبيعتها التي يمكن أن ترتكب بصور متعددة، ومن أماكن مختلفة، ومن بيئات يصعب اكتشافها أو السيطرة عليها، وإن مسألة مكافحتها تتطلب تظافر الجهود، سواء على المستوى الوطني، أو الدولي، من خلال إتباع آليات تساهم بشكل أو آخر في مواجهة هذه الجرائم، خاصة في ظل ما يشهده العالم من تطور علمي وتقني في مختلف الصعد، ومنها في الجانب المعلوماتي، عن طريق انتشار وسائل الاتصال الإلكتروني، من خلال شبكات الأنترنت، والذي بات من أهم وسائل التواصل في الوقت الحاضر، فضلاً عما خلفته جائحة كورونا من تداعيات في الجانب، وما صاحبها من تحول في أنماط التعامل اليومي، وإدارة المرافق العامة باستخدام تقنية المعلومات - الإدارة الإلكترونية للمرافق العامة -، وهذا الأمر

كانت له انعكاسات على الجانب الآخر، ألا وهو ظهور نوع جديد من الجرائم، وهو ما يعرف بالجرائم المعلوماتية، والتي بدأت هي الأخرى بالتنامي، مستغلين مرتكبيها، أو المروجين لها هذا الظرف، وتوظيف هذا التطور، وتلك التقنيات لتحقيق أغراض دنيئة، وربما ارتكاب جرائم أو أفعال تهدد الأمن العالمي من خلال القيام بهجمات سيبرانية قد تطال مسائل الدفاع في بعض الدول، أو توجيه هجماتها نحو المسائل المالية العالمية، مما يؤثر على الأمن المالي العالمي، لذلك لا بد من مكافحة هذه الجرائم، عن طريق آليات يجب أن تعتمد من الدول فراداً، أو مجتمعة لغرض منع وقعها، أو التقليل منها على أقل تقدير.

١,١.اهمية البحث: تتجلى أهمية موضوع البحث والدراسة، من خلال انتشار وتنامي الجرائم المعلوماتية على نطاق واسع، مما يتطلب وضع آليات لمكافحتها، أو الحد منها على أقل تقدير، سواء بوضع التشريعات التي تساهم في مكافحة تلك الجرائم، أو عن طريق ما تقوم به الأجهزة المعنية بمكافحة الجرائم، بما تمتلكه من وسائل، أو بما تقوم به من إجراءات، سواء في الشق الوقائي، أو العلاجي.

٢,١.أهداف البحث : تهدف الدراسة، إلى تبيان ماهية الجرائم المعلوماتية، وصورها، فضلاً عن بيان الآليات التي يمكن أن تتخذ في سبيل مكافحة الجرائم المعلوماتية، سواء ما تعلق منها بالجانب التشريعي، من خلال ما يضعه المشرع من قواعد قانونية تمكن الجهات المعنية بمكافحة تلك الجرائم، من الاضطلاع بمهامها في هذا الجانب، أو ما يتصل بالجانب التنفيذي، عن طريق ما تقوم به الإدارة ممثلة بأجهزتها الضبطية بما تقوم به من إجراءات في سبيل مكافحة هذا النوع من الجرائم.

٣,١.مشكلة البحث: تتمحور مشكلة البحث في محاولة الإجابة عن بعض التساؤلات : لعلَّ أهمها: ما المقصود بالجرائم المعلوماتية ؟ وما هي صورها أو أشكالها ؟ وما هي الآليات التي يمكن اتخاذها في سبيل مكافحة تلك الجرائم، ؟ وما هو الدور الذي يمكن أن تلعبه الإدارة في مكافحة تلك الجرائم ؟

٤,١. فرضية البحث : تنطلق فرضية البحث في وجود الجرائم المعلوماتية، وانتشارها بالشكل الذي أضحت تمثل ظاهرة عابرة للحدود، وترتكب من جانب أشخاص يجلسون خلف أجهزة الكومبيوتر، ويرتكبون جرائمهم بصورة سريعة جداً قد لا تستغرق أكثر من خطوة أو خطوتين، فهل تقف الدول مكتوفة الأيدي تجاه ذلك، وهل يمكن وضع آليات لمواجهتها، وتحديد مدى نجاعتها لمكافحة تلك الجرائم، أو الحد منها .

٥,١.منهج البحث: من أجل محاولة الإجابة عن التساؤلات التي أثرناها في مشكلة البحث، وفرضية البحث، فسنعمد إلى اتباع المنهج التحليلي، القائم على تحليل النصوص القانونية، وبحث الآراء الفقهية، والأحكام القضائية ذات الصلة بموضوع البحث.

٦,١.هيكلية البحث: للإلمام بجوانب هذا الموضوع، سنعمد إلى تقسيم بحثنا هذا على مبحثين: سنتناول في الأول بيان ماهية الجرائم المعلوماتية، وذلك بتقسيمه على مطلبين، الأول منها لتعريف الجرائم المعلوماتية، والثاني للحديث عن الطبيعة القانونية للجرائم المعلوماتية والأساس القانوني لمكافحتها، بينما سنخصص المبحث الثاني، للحديث عن آليات ودور الإدارة في مكافحة الجرائم المعلوماتية، وذلك بتقسيمه على مطلبين، سنتناول في الأول منه، الآليات الوقائية للإدارة لمكافحة الجرائم المعلوماتية، فيما نخصص الثاني الآليات العلاجية للإدارة لمكافحة الجرائم المعلوماتية ، ومن ثم نختم بحثنا بخاتمة تتضمن أهم الاستنتاجات التي سيتم التوصل إليها، وأهم المقترحات التي تخدم هذا الموضوع، وكما يلي:

٢.المبحث الأول: ماهية الجرائم المعلوماتية :

إن الحديث في الموضوع يتطلب تبيان مفهوم الجرائم المعلوماتية، كونها من الجرائم التي بدأت بالانتشار في الوقت الحاضر، وعدم وضع نظام قانوني لها، بسبب اختلاف النظرة إليها، علاوة اختلاف مستوى انتشارها بينها، كما أنها من الجرائم العابرة للحدود، وبالتالي فإن مسألة مواجهتها خاصة على الصعيد الدولي، ربما يؤدي إلى المساس بسيادة الدول، مما يجعل مسألة وضع تعريف جامع مانع لها محل خلاف وجدال بين الفقه، كما أن الحديث عن مكافحة تلك الجرائم، وضع آليات لمواجهتها يتطلب بيان الطبيعة القانونية لتلك الجرائم، ومن ثم بيان الأساس القانوني الذي ترتكز عليه مسألة مكافحة تلك الجرائم، ووفقاً لما تقدم وفي الإحاطة بجوانب هذا الموضوع، فإننا سنقسم هذا المبحث على مطلبين، سنتناول في الأول تعريف الجرائم المعلوماتية، فيما سنبين في الثاني طبيعة الجرائم المعلوماتية والأساس القانوني لمكافحتها، وكما يأتي:

١,٢.المطلب الأول: تعريف الجرائم المعلوماتية:

لقد اختلف الفقه والتشريعات في وضع تعريف جامع مانع لمفهوم أو مصطلح الجرائم المعلوماتية، وأول أوجه الاختلاف، هو الاختلاف في التسمية، فالبعض يطلق علياه تسمية الجرائم المعلوماتية، في حين هناك اتجاه آخر يطلق عليها تسمية الجرائم المعلوماتية، فقد عرفها البعض من زاوية النظر إلى أدوات استخدامها وهو جهاز الحاسوب، إذ يقصد بها" نشاط إجرامي يستخدم فيه تقنية الحاسب الآلي، بطرقة مباشرة أو غير مباشرة، كوسيلة لتحقيق أو تنفيذ الفعل الجرمي المقصود" وفقاً لما ذكره (حجازي، ٢٠٠٦)، وتعرف أيضاً من وجهة النظر هذه،" بأنها الجرائم التي تقع بواسطة الحاسب الآلي أو عليه أو بواسطة شبكة الأنترنت" (سلطان العلماء، ٥، ٢٠٠٥)، ومما يسجل على هذه التعريف هو التركيز على جانب الأنترنت والحاسوب، كأداة لارتكاب الجريمة، من التركيز دون التركيز على أغراضها، كما أن هناك من يخلط بينها وبين الجرائم الإلكترونية، إذ تعرف الجرائم الإلكترونية بأنها" فعل إجرامي يستخدم الحاسب في ارتكابه كأداة رئيسية" (باطلي، ١٦، ٢٠١٥) .

أما من جانبنا فيمكننا تعريف الجرائم المعلوماتية بأنها" الجرائم التي تستخدم تقنيات المعلومات والتطور التقني أساسا لتنفيذها، وتتخذ صوراً واشكلاً متعددة، وتستعمل الفضاء المعلوماتي العالمي مسرحاً له، بغض النظر عن دوافع وأهداف ارتكابها".

٢,٢. المطلب الثاني: الطبيعة القانونية للجرائم المعلوماتية وأساس مكافحتها:

كان موضوع الطبيعة القانونية للجرائم المعلوماتية، وأساس مكافحتها مدار خلاف وجدل بين الفقه، بسبب اختلاف نظرة كل منهم إلى هذا النوع من الجرائم، وكذلك بسبب التطور المتسارع لها، بما يحتم عدم استقرار الآراء بشأنها، وفي هذا المطلب سنتناول موضوع الطبيعة القانونية للجرائم المعلوماتية وأساس مكافحتها، وذلك بتقسيمه على فرعين، نخصص الأول منه للحديث عن الطبيعة القانونية للجرائم المعلوماتية، والثاني لبيان أساس مكافحتها، وعلى النحو الآتي:

١,٢,٢. الفرع الأول: الطبيعة القانونية للجرائم المعلوماتية:

كما اسلفنا في بداية حديثنا في هذا المطلب، من عدم اتفاق الفقه بشأن الطبيعة القانونية للجرائم المعلوماتية، فقد ذهب جانب من الفقه بالقول أن الجرائم المعلوماتية تعد ظاهرة إجرامية ذات طبيع خاصة تتعلق بالقانون الجنائي المعلوماتي،

كونها هذه الجرائم ترتكب ضمن نطاق المقومات والتقنيات الإلكترونية، وفقاً لما ذكره (أبو عامر و القهوجي، ١٩٩٣)، في حين ذهب جانب آخر من الفقه إلى القول بأن الجرائم المعلوماتية ذو طبيعتين مختلفتين، الأولى تتمثل بالجانب المادي، كحالة تخزين المعلومات في جهاز الحاسوب، أو على أقراص، وأشياء مادية، والثاني غير مادي، أي بمعنى وجود شيء ملموس مادياً كحالة انتقال المعلومات، وبالتالي فإن الجرائم المعلوماتية تخض لأكثر من نظام قانوني، ذكره(حسن، ١٩٩٩)، في حين يذهب جانب آخر منش الفقه إلى القول بأن الجرائم المعلوماتية، هي جرائم ذات طبيعة متعدية الحدود، كونها لا تقتصر على دولة معينة، بل أنها عابرة للحدود، ذكره (قوره، ٢٠٠٥)، ووفقاً لما تقدم يمكن القول بأنه لا يوجد إجماع لدى الفقه بشأن الطبيعة القانونية للجرائم المعلوماتية، لكننا نرى بأن الأقرب هو أنها ذات طبيعة خاصة.

٢,٢,٢. الفرع الثاني: أساس مكافحة الجرائم المعلوماتية:

إن مكافحة الجرائم المعلوماتية لن تكون ذات جدوى، ولا يمكن تحقيقها، من دون وجود تعاون وطني ودولي، ومن دون ذلك التعاون على المستويين الوطني والدولي فلن يأتي بأية نتائج ملموسة تساهم أو تحد من تلك الجرائم ، خاصة إذا ما علمنا بأنها "جرائم عابرة للحدود"، إذ أنها لا تقتصر على دولة بعينها، أو ينحصر تأثيرها في تلك الدولة، بل أن تلك الجرائم ترتكب عبر - دولة أو مجموعة دول - لكن آثارها تمتد لتصل إلى عدد غير محدود ن الدول، وعليه فإن الأساس الذي ترتكز عليه مسألة مكافحة الجرائم المعلوماتية، هو التعاون الوطني والدولي وتنسيق الجهود المبذولة بين كافة الدول، من أجل تحقيق نتائج مهمة ومثمرة، يمكن الارتكاز عليها، وتقويتها للحد من آثار تلك الجرائم على العالم بأسره، ذكره (الكعبي، ٢٠٠٩)، وهذا يتطلب وجود أساس يرتكز عليه موضوع مكافحة الجرائم المعلوماتية، وهو ما سنبينه في هذا الفرع، إن مسألة مكافحة الجرائم المعلوماتية على المستوى الوطني، يتطلب وجود نصوص قانونية تستند إليها الأجهزة المهنية بهذا الأمر، ففي ما يتعلق بموقف المشرع الدستوري، نجد أن دستور العراق لعام ٢٠٠٥، قد نص على حقوق وحريات الأفراد، إذ نص في المادة (١٧/أولاً) على حقوق الأفراد في الحقوق الشخصية، وبما لا يتنافى مع حقوق الآخرين والآداب العامة " لكل فرد الحق في الخصوصية الشخصية بما لا يتنافى مع حقوق الآخرين والآداب العامة، " في حين نص في المادة (٤٠) على حرية الاتصالات والمراسلات البريدية والهاتفية والإلكترونية، إذ جاء فيها ما نصه "حرية الاتصالات والمراسلات البريدية والبرقية والهاتفية والإلكترونية وغيرها مكفولة، ولا يجوز مراقبتها أو التنصت عليها، أو الكشف عنها، إلا لضرورةٍ قانونيةٍ وأمنية، وبقرارٍ قضائي"، ومن نص هذه المادة الدستورية، نجد أن المشرع الدستوري، قد أجاز مكافحة الجرائم المعلوماتية، ولكنه قيدها بشروط، وهي الضرورات القانونية والأمنية، وأن تكون بقرار قضائي".

أما على صعيد التشريعات العادية ففي قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩ المعدل، نجد أن المشرع العراقي لم يتطرق بصورة صريحة إلى الجرائم المعلوماتية لاختصاص الشامل، مادة ١٣ في غير الأحوال المنصوص عليها في المواد ٩ و١٠ و١١ تسري أحكام هذا القانون على كل من وجد في العراق بعد أن ارتكب في الخارج بوصفه فاعلا أو شريكا جريمة من الجرائم التالية: تخريب أو تعطيل وسائل المخابرات والمواصلات الدولية والإتجار بالنساء أو بالصغار أو بالرقيق أو بالمخابرات "، ومن نص هذه المادة يتضح بأن المشرع العراقي منح الأجهزة المعنية بمكافحة الجرائم المعلوماتية اتخاذ ما يلزم بشأن مكافحة تلك الجرائم، بل أن المشرع العراقي لم يشترط ارتكاب الجريمة داخل العراق من أجل ملاحقة مرتكبها واتخاذ الإجراءات القانونية بحقه، بل حتى لو ارتكبت خارج العراق، ذكره (سالم، ٢٠٢١)، أما قانون مكافحة الإرهاب رقم ١٣ لسنة ٢٠٠٥، فإنه لم ينص على مكافحة الجرائم المعلوماتية، كما سعى العراق لتشريع قانون الجرائم المعلوماتية لكنه واجه معارضة سياسية وشعبيه، ونأمل من المشرع الإسراع في تشريع

القوانين وبالشكل الذي يحقق نوعاً من التوازن بين حقوق وحريات الأفراد، والحد من الجرائم المعلوماتية، يضاف إلى ذلك فإن المشرع العراقي قد صادق إلى الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠، وذلك بموجب القانون رقم (٣١) لسنة ٢٠١٣، وهذه الاتفاقية تلزم الدولة العراقية مكافحة الجرائم المعلوماتية، طبقاً لما نص عليه (الفصل الثاني) من هذه الاتفاقية.

٣. المبحث الثاني: آليات الإدارة لمكافحة الجرائم المعلوماتية:

كما اسفنا في بداية حديثنا في هذا الموضوع بأن مكافحة الجرائم المعلوماتية لا يمكن تحقيقه إلا من خلال تظافر الجهود على المستوى الوطني والدولي، كونها من الجرائم العابرة للحدود، وأن مكافحتها على الصعيد الوطني يقع على عاتق الإدارة، بما تمتلكه من أدوات ووسائل تلجأ إليها للقيام بهذه المهمة على الوجه الأكمل، لذلك لا بد من وجود آليات تمكن الإدارة الاضطلاع بذلك، وتلك الآليات البعض منها وقائي تمارسه الإدارة لمنع وقوع تلك الجرائم، والبعض الآخر علاجي تقوم به الإدارة بعد وقوع تلك الجرائم واتخاذ الإجراءات القانونية بحق مرتكبيها، وفي هذا المبحث سنبين تلك الآليات، ودور الإدارة في مكافحة الجرائم المعلوماتية والحد منها، من خلال تقسيم هذا المبحث على مطلبين، سنتناول في الأول الآليات الوقائية لمكافحة الجرائم المعلوماتية، والثاني للحديث عن الآليات العلاجية لمكافحة الجرائم المعلوماتية، وكما يلي:

١,٣.المطلب الأول: آليات الإدارة الوقائية لمكافحة الجرائم المعلوماتية:

الأصل بإجراءات الإدارة في مسألة حفظ النظام العام بعاصره المختلفة، ومن بينها عنصر الأمن، والذي قد يعكر صفوه الجرائم المعلوماتية هو الصفة الوقائية، لذلك فإن هناك عدة آليات يمكن أن تلجأ إليها الإدارة في سبيل الوقائية من الجرائم المعلوماتية، ومنع وقوعها، وتتمثل تلك الآليات بالآتي:

١,١,٣. المراقبة الإلكترونية: لما كانت وظيفة الضبط الإداري تتسم بالصفة الوقائية، فإن حفظ الأمن العام في الفضاء الإلكتروني، ومنها مكافحة الجرائم المعلوماتية، يستلزم قيام الإدارة بإتباع المراقبة الإلكترونية لمواقع التواصل الاجتماعي التي قد تنشر الأخبار والشائعات المهددة الأمن العام، ذكره (الداودي، ٢٠٠٧)، والمراقبة التي تتم باستخدام الحاسوب من خلال الحاسوب على نشاط إلكتروني معين، وفقاً لما ذكره (زينو، ٢٠١٧)، وتمثل المراقبة الإلكترونية إحدى الآليات أو التدابير الاحترازية التي تتولاها الإدارة من خلال أجهزة الضبط الإداري المختصة، ويقصد بالمراقبة الإلكترونية العمل الذي يقوم به المراقب باستخدام التقنية الإلكترونية لجمع البيانات والمعطيات من المشتبه بهم، وينبغي القول هنا إن مراقبة الاتصالات سواء كانت الكرتونية أم هاتفية تمثل من حيث المبدأ انتهاكاً لحرية الاتصالات التي أكدت عليها الدساتير، ومن بينها الدستور العراقي لعام ٢٠٠٥، والذي نص في المادة(٤٠) منه على أن "حرية الاتصالات والمراسلات البريدية والبرقية والهاتفية والإلكترونية وغيرها مكفولة، ولا يجوز مراقبتها أو التنصت عليها، أو الكشف عنها، إلا لضرورةٍ قانونيةٍ وأمنية، وبقرارٍ قضائي" ومن نص هذه المادة الدستورية، نجد أن المشرع الدستوري، قد أجاز مكافحة الجرائم المعلوماتية، ولكنه قيدها بشروط، وهي الضرورات القانونية والأمنية، وأن تكون بقرار قضائي" ذكره (الحمداني، ٢٠٢٠)، وقد جاء في قانون جهاز مكافحة الإرهاب رقم ٣١ لسنة ٢٠١٦، يسعى الجهاز إلى تحقيق أهدافه بالوسائل التي نصت عليها المادة (الثالثة) والتي جاء فيها " ثانيا : تنفيذ العمليات الأمنية والخطط الاستراتيجية فيما يتعلق بفعاليات مكافحة الإرهاب وله في سبيل ذلك وفقا للقانون : أ ـ تنفيذ عمليات المراقبة التفتيش والتحري بناءً على امر قضائي. ب ـ

مراقبة الاتصالات ومواقع التواصل الاجتماعي والمواقع الإلكترونية بناء على أمر قضائي". ويذهب البعض من الباحثين إلى ضرورة إيجاد نوع من التوازن بين حرية الأفراد في تداول المعلومات ونشرها على مواقع الأنترنت المختلفة وبين سلطات الضبط الإداري عندما تمارس وظيفة المراقبة الإلكترونية، ذكرته (مصطفى).

٢,١,٣. الترخيص الإلكتروني: يعد الترخيص الإلكتروني من بين الآليات الوسائل التي يمكن للإدارة اللجوء إليها، من أجل مواجهة ومكافحة الجرائم المعلوماتية، وذلك من خلال تحديد الأنشطة الإلكترونية وضبطها، ويتمثل ذلك في صورة إجراءات تقييدية تفرضها الإدارة على الأفراد، قبل القيام بالنشاط، وذلك بالحصول على الترخيص أو الإذن المسبق من جهات الضبط الإداري المعنية بذلك، وتملك سلطات الضبط الإداري المختصة سلطة تقديرية في منح ذلك التراخيص من عدمه، وفقا لما تراه، وتكون قراراتها في هذا الطاق خاضعة لرقابة القضاء الإداري، ذكره (خليل، ٢٠١٩)، ويتيح الترخيص للأشخاص الذين تتوفر فيهم الشروط المطلوبة من إنشاء واستغلال الشبكات المعلوماتية، أو تقديم خدمات معينة، لذلك فالترخيص الإلكتروني يُمكِنْ سلطة الضبط الإداري من ممارسة رقابة صارمة على إنشاء واستغلال خدمات الإنترنت، وهي نشاطات حساسة تخضعها سلطة الضبط الإداري لشروط دقيقة ومحددة، ودراسة مفصلة وشاملة، وبناءً عليها تقبل ممارستها من طالب الترخيص أو ترفض ذلك.

ويذكر (البسيوني، ٢٠٠٨) ، "أنه لا يجوز للائحة أن تشترط ضرورة الحصول على ترخيص سابق فيما يتعلق بممارسة الحريات العامة التي يكفلها الدستور والقانون، وعلى ذلك إذا نص الدستور أو القانون على ضمان حرية من الحريات دون أن يخضع النشاط المتعلق بهذه الحرية لنظام الترخيص، فإنه لا يجوز لجهة الإدارة أن تفرض هذا النظام وإلا كان تصرفها غير مشروع ، أما إذا كانت الحريات لا يكفلها الدستور أو القانون، والتي يطلق عليها الحريات غير المعروفة أو المحددة وهي تتعلق في الغالب بغير الحريات الأساسية ، فإن الإدارة تستطيع أن تفرض نظام الترخيص لممارسة هذا النوع من الحريات، ويجب على سلطة الضبط أن تفرض نظام الترخيص بطريقة موضوعية خالصة، بحيث تحدد الشروط والضوابط بطريقة عامة ومجردة، فيمنح لكل من تتوفر فيه الشروط من غير تمييز، كما يجب أن يكون استعمالها لهذه السلطة بالقدر الضروري، وإلا كان استعمالها غير مشروع، ويخضع لرقابة القضاء" .

٣,١,٣. إنشاء مركز شرطة إلكتروني متخصص بمكافحة الجرائم المعلوماتية : إن التقدم المتواصل في تكنولوجيا المعلومات، والحاسب الآلي والإنترنت ، يفرض على الدول أن تسير في خطوات متناسقة مع التطورات السريعة التي تشهدها هذه التقنيات، والإلمام بها، كي يمكن التصدي للأفعال الإجرامية، التي صاحبت هذه التكنولوجيا ومواجهتها هذا من ناحية، ومن ناحية أخرى فإن إعمال القانون في مواجهة الجرائم المعلوماتية يستلزم اتخاذ إجراءات قد تتجاوز المفاهيم والمبادئ المستقرة في المدونة العقابية التقليدية، لما يتسم به هذا النوع الجرائم من حداثة في الأسلوب، وسرعة في التنفيذ وسهولة في إخفائها والقدرة على محو آثارها، وإنشاء مركز شرطة إلكتروني، متخصصة للتحقيق في الجرائم المعلوماتية، ويفضل أن يكون العاملين عليها من المحققين ذوي الإلمام بجهاز الحاسوب، وكذلك لديهم القدرة على التعامل مع أجزاءه، ومن خلال إنشاء هذا المركز تستطيع الإدارة أن تحد من الجرائم المعلوماتية، كونه سيكون مركز متخصص بهذا النوع من الجرائم.

٢,٣.المطلب الثاني: آليات الإدارة العلاجية لمكافحة الجرائم المعلوماتية:

فيما يتعلق بالآليات العلاجية التي تتخذها الإدارة في مكافحة الجرائم المعلوماتية، فإن هناك عدة آليات تتخذها في سبيل تحقيق تلك الغاية أو الهدف، وتتلخص بالآتي:

١,٢,٣. الحظر والحجب الإلكتروني: يقصد بالحجب الإلكتروني، إجراء تقوم به الأجهزة المختصة بمساعدة مقدمي الخدمات الوسيطة عادة، تمنع من خلاله المستخدمين في نطاق جغرافي معين، من الوصول إلى موقع أو أكثر من المواقع على الشبكة العنكبوتية، ومواقع التواصل الاجتماعي، بصفة دائمة أو مؤقتة، من أجل حماية النظام العام بعناصره المختلفة، فيهدف المواجهة المستعجلة للمضامين، والأنشطة المحظورة المتعلقة خصوصا بنشر مواد إباحية للأطفال، بالإرهاب أو بجرائم الكراهية، يمكن لسلطات الضبط الإداري في العديد من الدول أن تصدر قرار حجب موقع معين دون الحاجة لقرار قضائي بذلك، إذ تملك الإدارة صلاحية مطالبة مزودي الخدمات بحظر الوصول الموقع أو أكثر دون ضرورة إبلاغ متعدي الإيواء في البلدان الأخرى، ذكره (Conseil de l'Europe ، 2017)، ويمكن لأجهزة الضبط الإداري المعنية بمكافحة الجرائم المعلوماتية، القيام بعدة إجراءات ذات الصلة بموضوع الحظر الإلكتروني، ومنها تدابير حجب مواقع شبكات التواصل الاجتماعي الإلكترونية، ويعد الحجب من بين أكثر تدابير الضبط الإداري الإلكتروني، تعرضا للنقد نظرا لكونه يماثل فكرة الحظر من حيث أنه من التدابير الوقائية المانعة لممارسة النشاط، بهدف فهم شامل الحجب نطرق أولا لمفهومه، لتبحث بعد ذلك في أساليب تطبيقه .

٢,٢,٣. التفتيش الإلكتروني: يقصد بالتفتيش الإلكتروني، الوصول إلى تحويه نظم الحاسوب الآلي، من أشياء مادية ومعنوية، تفيد في الكشف عن الحقيقية، ونسبتها إلى المتهم مرتكب الجريمة المعلوماتية، ذكره (الطوالبة، ٢٠٠٤)، كما يعرف بأنه الاطلاع على محل منحه القانون حماية خاصة بوصفه مستودع سر صاحبه، ويستوي أن يكون ذلك المحل، جهاز الحاسوب الآلي، أو نظمه، أو شبكة الأنترنت، ذكرته (هروال، ٢٠٠٧)، ولخطورة التفتيش الإلكتروني، لصلته المباشرة بالخصوصية والحرية الشخصية للشخص المزمع إجراء التفتيش عليه، فإنه يشترط توافر عدة شروط فيه، منها، وقوع جريمة ذات صلة بالجرائم المعلوماتية، وأن يكون الشخص المالك للوسيلة الإلكترونية مشتبهاً به بصفته فاعلاً أو مساهماً في ارتكاب الجريمة، ووجود أدلة قوية إلكترونية تساهم في إمكانية الوصول إلى الحقيقة، وأن يجري التفتيش من الجهة المختصة به قانوناً ووفقاً لقرار قضائي، ذكره (العدوان و السلامات، ٢٠١٨)، ولقد نص المشرع العراقي على انه لا يجوز تفتيش الأشخاص أو الأماكن إلا إذا كان الشخص متهماً بارتكاب جريمة، ولم يحدد المشرع العراقي نوع الجريمة المرتكبة ويعني ذلك أن التفتيش جائز في جميع أنواع الجرائم، الجنايات، الجنح، والمخالفات، وعن طريق التفتيش الإلكترونية، يمكن للإدارة الحد من الجرائم المعلوماتية.

٣,٢,٣. الجزاء الإداري: يعد الجزاء الإداري من بين الآليات التي يمكن أن تلجأ إليها الإدارة في سبيل مواجهة الجرائم المعلوماتية، ووفقاً لما ذكرت (الشرقاوي، ١٩٨٣)، بأنه يمكن للإدارة عن طريق أجهزة الضبط الإداري، أن تلجأ إلى الجزاءات الإدارية المختلفة، ومنها ما يكون مالياً كالمصادرة، أو مهنياً كسحب الترخيص، أو الإغلاق المؤقت والنهائي للمحل مرتكب الفعل، أو الذي قام بالنشاط المخالف ، ويذكر (جلطي، ٢٠١٦) بأن الجزاء الإداري تقوم به السلطات الإدارية في حال مخالفة الشخص للقواعد التي تنظم نشاطاً معيناً، والجزاءات الإدارية تفرضها الإدارة على الأفراد أو المؤسسات، بإرادتها المنفردة، ومن دون تدخل القضاء عند ارتكابهم فعلاً مخالفاً، أو الاعتداء على مصلحة يحميها القانون، وفي مجال مكافحة الجرائم المعلوماتية، يمكن للإدارة استخدام هذا الجزاء في سبيل مكافحة الجرائم المعلوماتية، أو الحد منها.

٤. الخاتمة:

بعد نهاية كتابة بحثنا هذا، فقد توصلنا عدة استنتاجات، فضلاً عن العديد من والتوصيات التي نراها جديرة بالذكر، التي نأمل أن يتم تطبيقها، بالشكل الذي يعزز دور الإدارة في مكافحة الجرائم المعلوماتية، وعلى النحو الآتي:

١,٤. الاستنتاجات: لقد توصلنا في بحثنا هذا استنتاجات عدة، من ابرزها ما يلي:

١,١,٤. إن الجرائم المعلوماتية تعد من الجرائم العابرة للحدود، ولم تتفق التشريعات أو الفقه، سواء على الصعيد الدولي أو الوطني على وضع تعريف جامع مانع لها.

٢,١,٤. إن مكافحة الجرائم المعلوماتية يتطلب تظافر جهود الدول مجتمعة، علاوة على الجهود التي تفرض من جانب الدول فراداً، ويتطلب تعاون دولي بهذا الخصوص، في سبيل مكافحتها أو الحد منها على أقل تقدير.

٣,١,٤. هناك جملة من الآليات الوقائية التي يمكن للإدارة اللجوء إليها في سبيل مكافحة الجرائم المعلوماتية على الصعيد الوطني، وتتمثل تلك الآليات، الترخيص الإلكتروني، والمراقبة الإلكترونية، وإنشاء مركز شرطة متخصص بمكافحة الجرائم المعلوماتية.

٤,١,٤. توجد عدة آليات علاجية تقوم بها الإدارة في سبيل مواجهة الجرائم المعلوماتية، منها، الحظر الإلكتروني، والتفتيش الإلكتروني، والجزاءات الإدارية التي تفرض على المخالفين.

٥,١,٤. لقد عالج المشرع العراقي موضوع مكافحة الجرائم المعلوماتية، في قوانين متفرقة، سواء بصورة مباشرة أو غير مباشرة، بسبب عدم تشريع قانون مكافحة الجرائم المعلوماتية لغاية الآن، ومنها قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩ المعل، وقانون مكافحة الإرهاب رقم ١٣ لسنة ٢٠٠٥.

٢,٤. التوصيات: وفقاً للاستنتاجات التي ذكرناه آنفاً، فإننا نوصي بالآتي:

١,٢,٤. نوصي المشرع العراقي بضرورة الإسراع بتشريع قانون مكافحة الجرائم المعلوماتية، لما له من دور في منح الإدارة الدور الفَعّال في مكافحة الجرائم المعلوماتية.

٢,٢,٤. نوصي الحكومة العراقية عن طريق وزارة الداخلية، والجهات ذات الصلة بمكافحة الجرائم المعلوماتية، بالعمل على إنشاء مركز شرطة متخصص في مكافحة الجرائم المعلوماتية.

٣,٢,٤. تدريب الكوادر العاملة على مكافحة الجرائم المعلوماتية، على الوسائل والأساليب الاتي تساعدهم في إداء مهامهم الوظيفية ذات الصلة بمكافحة الجرائم المعلوماتية.

٤,٢,٤. التنسيق المستمر مع الدول في مجال مكافحة الجرائم المعلوماتية، والاستفادة من تجارب الدول الرائدة في المجال بما يساهم في مكافحة هذا النوع من الجرائم.

٥,٢,٤. على الإدارة توخي الحذر والدقة عند اتخاذها الإجراءات اللازمة لمكافحة الجرائم المعلوماتية، بالشكل الذي يحقق نوعاً من التوازن بين حقوق وحريات الأفراد في المجال الشخصي، وبين محاربة الجرائم من هذا النوع.

٥. المصادر والمراجع:

١,٥. الكتب:

١,١,٥. د. أبو عامر، محمد زكي و د. القهوجي، علي عبد القادر . قانون العقوبات القسم الخاص. دار النهضة العربية، القاهرة.(١٩٩٣).

٢,١,٥. د. البسيوني، عبد الرؤوف هاشم. نظرية الضبط الإداري في النظم الوضعية المعاصرة والشريعة الإسلامية. ط١. دار الفكر الجامعي. الإسكندرية.(٢٠٠٨).

٣,١,٥. الداودي، محمد عبد الكريم حسين. المسؤولية الجنائية لمورد خدمه الإنترنت. منشورات الحلبي الحقوقية. بيروت.(٢٠٠٧).

٤,١,٥. الطوالبه، حسن. التفتيش الجنائي على نظم الحاسوب والأنترنت. عالم الكتب الحديثة. اربد.(٢٠٠٤).

٥,١,٥. الكعبي، محمد عبيد. الجرائم الناشئة عن الاستخدام الغير مشروع لشبكة الأنترنت. دار النهضة العربية. (٢٠٠٩).

٦,١,٥. جلطي أعمر: الأهداف الحديثة للضبط الإداري، أطروحة دكتوراه ، كلية الحقوق السياسية، جامعة أبي بكر بلقايد تلمسان، ٢٠١٦

٧,١,٥.حجازي، عبد الفتاح بيومي. مكافحة جرائم الكمبيوتر والأنترنت في القانون العربي النموذجي. دار الفكر الجامعي. الإسكندرية.(٢٠٠٦).

٨,١,٥. د. حسن، سعيد عبد اللطيف. إثبات جرائم الكومبيوتر والجرائم المرتكبة عبر الأنترنت. دار النهضة العربية. القاهرة.(١٩٩٩).

٩,١,٥. خليل، مصطفى طالع. التنظيم القانوني لحرية الأعلام المرئي والمسموع. المركز العربي للنشر والتوزيع. القاهرة.(٢٠١٩).

١١,١,٥. د. راضي، مازن ليلو. القانون الإداري - دراسة عامة الأسس والمبادئ القانون الإداري في العراق. مطبعه هاوار. دهوك. (٢٠٠٧).

١٢,١,٥. د. سعاد الشرقاوي. القانون الإداري. دار النهضة العربية. القاهرة. (١٩٨٣).

١٣,١,٥. سلطان العلماء، محمد عبد الرحيم. جرائم الأنترنت والاحتساب عليها. بحث مقدم مؤتمر القانون والكمبيوتر والأنترنت. جامعة الإمارات.(٢٠٠٥).

١٤,١,٥. غنية، باطلي. الجريمة الإلكترونية – دراسة مقارنة. منشورات الدار الجزائرية. الجزائر.(٢٠١٥).

١٥,١,٥. د. قوره، نائله. جرائم الحاسب الآلي الاقتصادية. منشورات الحلبي. بيروت. (٢٠٠٥).

١٦,١,٥. د.موسى، مصطفى محمد . المراقبة الإلكترونية عبر شبكه الأنترنت بين المراقبة الأمنية التقليدية والإلكترونية. دار الكتب الوثائق المصرية. القاهرة.(٢٠٠٣).

١٧,١,٥. هروال، نبيله هبة. الجوانب الإجرائية لجرائم الأنترنت. دار الفكر الجامعي. الإسكندرية.(٢٠٠٧).

٢,٥. الرسائل الجامعية:

١,٢,٥. زينو، مصطفى جمال حنفي. دور الضبط الإداري في مجال الجرائم الإلكترونية المخلة في الأمن العام- دراسة تحليلية. رسالة ماجستير. جامعه الأزهر. غزه.(٢٠١٧).

٣,٥. البحوث والدراسات:

١,٣,٥. د. الحمداني، سامي حسن نجم . دور الضبط الإداري الإلكتروني في مكافحة الشائعات المخلة بالأمن العام. بحث منشور مجلة جامعة تكريت للحقوق. العدد١. المجلد ٥. الجزء١. السنة ٥ . (٢٠٢٠).

٢,٣,٥. العدوان، ممدوح حسن مانع و السلامات، نادر عبد الحليم . مشروعية وحجية الدليل المستخلص من التفتيش الإلكتروني في التشريع الجزائي الأردني. بحث منشور. مجلة دراسات للعلوم الشرعية والقانون. المجلد ٤٥.العدد ٤.الملحق ٢.(٢٠١٨).

٣,٣,٥. . د.سالم، طاهر خلف. مكافحة الجرائم المعلوماتية لضمان تعزيز الأمن المجتمعي في منظور القانون الدولي. بحث. مجلة جامعة تكريت للحقوق.السنة٦.المجلد ٦.العدد ٢. الجزء ٢.(٢٠٢١).

٤,٥. الدساتير والتشريعات:

١,٤,٥. الدساتير:

١,١,٤,٥. دستور جمهورية العراق لعام ٢٠٠٥.

٢,٤,٥. التشريعات:

١,٢,٤,٥. قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩ المعدل.

٢,٢,٤,٥. قانون أصول المحاكمات الجزائية العراقي رقم ٢٣ لسنة ١٩٧٩ المعدل.

٣,٢,٤,٥. قانون مكافحة الإرهاب العراقي رقم ١٣ لسنة ٢٠٠٥.

٥,٥. المصادر من الأنترنت:

١,٥,٥. مصطفى، زينة عبد هللا. الرقابة الإلكترونية وحريه الراي والتعبير. مقال المنشور على الموقع الإلكتروني الخاص بالمركز العربي لأبحاث الفضاء الإلكتروني على الرابط www.acsronline.comlartile.defail.aspxjid=258955 تاريخ الزيارة ٢٠٢٢/٦/١٥ .

٦,٥. المصادر الأجنبية:

1.6.5. Conseil de l’Europe, l'Étude comparative sur le blocage. le filtrage et le retrait de contenus illegaux sur internet. Lausanne.(2017).

5. Sources and references:

5.1. books:

5.1.1.Dr.. Abu Amer, Muhammad Zaki and Dr. Al-Qahwaji, Ali Abdel-Qader. Penal Code Special Section. Arab Renaissance House, Cairo. (1993.(

5.1.2 .Dr.. Bassiouni, Abdel Raouf Hashem. Administrative Control Theory in Contemporary Positive Systems and Islamic Law. i 1. University Thought House. Alexandria. (2008.(

5.1.3 .Daoudi, Muhammad Abdul Karim Hussein. Criminal liability of the Internet service provider. Al-Halabi Publications. Beirut. (2007.(

5.1.4. Tawalbeh, Hassan. Forensic inspection of computer systems and the Internet. The world of modern books. Irbid. (2004.(

5.1.5. Al-Kaabi, Mohammed Obaid. Crimes arising from the illegal use of the Internet. Arab Renaissance House. (2009.(

5.1.6. Galati Amar: Modern Objectives of Administrative Control, PhD Thesis, Faculty of Political Law, University of Abu Bakr Belkaid Tlemcen, 2016

5.1.7. Hegazy, Abdel Fattah Bayoumi. Combating computer and internet crimes in the Arab Model Law. University Thought House. Alexandria. (2006.(

5.1.8. Dr.. Hassan, Saeed Abdul Latif. Proof of computer crimes and crimes committed via the Internet. Arab Renaissance House. Cairo. (1999.(

5.1.9. Khalil, Mustafa Tala'. Legal regulation of freedom of audiovisual media. Arab Center for Publishing and Distribution. Cairo. (2019.(

5.1.10.Dr.. Radi, Mazen Lilo. Administrative Law - General Study Foundations and Principles of Administrative Law in Iraq. Hawar Press. Dohuk. (2007.(

5.1.11. Dr.. Souad Al-Sharqawi. Administrative Law. Arab Renaissance House. Cairo. (1983.(

5.1.12. Sultan Al-Ulama, Muhammad Abdul Rahim. Internet crimes and counting them. Research presenter conference law, computer and the Internet. Emirates University. (2005.(

5.1.13.Rich, void. Cyber crime - a comparative study. Algerian House Publications. Algeria. (2015.(

5.1.14.Dr.. Qora, Naila. Economic computer crimes. Al-Halabi Publications. Beirut. (2005.(

5.1.15. Dr. Mousa, Mustafa Mohamed. Electronic monitoring via the Internet between traditional and electronic security monitoring. Egyptian Documents Book House. Cairo. (2003.(

5.1.16.Harwal, Nabila Heba. Procedural aspects of Internet crimes. University Thought House. Alexandria. (2007.(

5.2.Undergraduate theses:

5.2.1.Zeno, Mustafa Gamal Hanafi. The role of administrative control in the field of cybercrime against public security - an analytical study. Master Thesis. Al Azhar university. Gaza.(2017.(

5.3.Research and Studies:

5.3.1. Dr.. Al-Hamdani, Sami Hassan Najm. The role of electronic administrative control in combating rumors that disturb public security. Research publication of the Journal of Tikrit University of Law. Issue 1. Volume 5. Part 1. year 5. (2020.(

5.3.2. Aggression, Mamdouh Hassan Manea and Salamat, Nader Abdel Halim. Legality and Authenticity of Evidence Extracted from Electronic Inspection in Jordanian Penal Legislation. Posted search. Studies magazine for forensic sciences and law. Volume 45. Issue 4. Supplement 2. (2018.(

5.3.3. Dr. Salem, Taher Khalaf. Combating cybercrime to ensure the strengthening of societal security in the perspective of international law. Search. Tikrit University Journal of Law. Year 6. Volume 6. Issue 2. Part 2. (2021.(

5.4.Constitutions and Legislation:

5.4.1. Constitutions:

5.4.1.1. Constitution of the Republic of Iraq for the year 2005.

5.4.2. Legislation:

5.4.2.1.Iraqi Penal Code No. 111 of 1969 amended.

5.4.2.1.The Iraqi Code of Criminal Procedure No. 23 of 1979, as amended.

5.4.2.2.Iraqi Anti-Terror Law No. 13 of 2005.

5.5.Sources from the internet:

5.5.1. Mustafa, Zina Abdullah. Electronic censorship and freedom of opinion and expression. Article published on the website of the Arab Center for Cyberspace Research at the link www.acsronline.comlartile.defail.aspxjid=258955, date of visit 15/6/2022.