جامعة الشارقة
UNIVERSITY OF SHARJAH

جامعة الشارقه – كلية القانون

برنامج الدكتوراه في القانون العام.

خصوصية التحقيق في جرائم أمن الدولة المعلوماتي

دراسة مقارنة

تقديم الباحث

محمد عبدالله سليمان الظهوري

الرقم الجامعي : U 20106155

اسم المشرف الدكتور

محمد نورالدين سيدي

استاذ مشارك كلية القانون جامعة كلباء

ملخص

يهدف البحث لبيان خصوصية التحقيق في جرائم أمن الدولة المعلوماتي من خلال بيان تعريف التحقيق في هذه الجرائم، والجهة المختصة بالتحقيق بجرائم امن الدولة المعلوماتي في دولة الإمارات العربية المتحدة، وبيان التحديات التي تواجه التحقيق لفي هذه الجرائم.

تتمثل أهمية البحث من الناحية العلمية في أنه من أوائل البحوث المتخصصة التي تتناول موضوعاً في غاية الأهمية هو خصوصية التحقيق في جرائم أمن الدولة المعلوماتي، وخاصة ان المشرع الإماراتي استحدث قانونا خاصا بمكافحة الجرائم الإلكترونية، هو المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ بشأن مكافحة الشائعات والجرائم الإلكترونية، الذي تضمن نصوصاً خاصة بالتحقيق في هذا النوع من الجرائم، وأفرد مواد خاصة للتجريم والعقاب على الجرائم التي تستهدف أمن الدولة المعلوماتي.

وعليه فإن البحث يعتبر ركيزة أساسية في تناوله لجزئية محددة في مكافحة جرائم امن الدولة المعلوماتي، وهو التحقيق، وذلك لما للتحقيق من أهمية كبيرة في استجلاء الأدلة وإسناد الجريمة لمرتكبها نظراً لما تشكله جرائم أمن الدولة المعلوماتي من خطر على المجتمع والامن.

وعليه فإن مشكلة الدراسة تكون ذات بعدين، البعد الأول هو تعدد جهات الاختصاص في التحقيق في جرائم أمن الدولة المعلوماتي، بين نيابة أمن الدولة وبين النيابة الاتحادية لجرائم الشائعات والجرائم الإلكترونية، وهذا التعدد في الاختصاص له العديد من الآثار السلبية في التحقيق في الجرائم التي تمس أمن الدولة المعلوماتيز

أما البعد الثاني من المشكلة هو الصعوبات التي تواجه جهة التحقيق في جرائم امن الدولة المعلوماتي من حيث سرعة طمس معالم الجريمة وصعوبة معرفة مرتكبها، والبعد المكاني لارتكاب الجريمة، وعليه يمكن بلورة مشكلة البحث في التساؤل التالي: ما مدى كفاية التشريعات الإجرائية الإماراتية في الإحاطة بخصوصية جرائم امن الدولة المعلوماتي؟

ومن أبرز نتائج البحث :إن التحقيق في جرائم امن الدولة المعلوماتي له خصوصية يتميز بها عن التحقيق التقليدي، ويكتسب هذه الخصوصية من حيث طبيعة جرائم أمن الدولة المعلوماتي التي نص عليها المشرع الإماراتي في مرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ بشأن مكافحة جرائم الشائعات والجرائم الإلكترونية، كما ان خصوصية التحقيق في جرائم أمن الدولة المعلوماتي تظهر من خلال طبيعة الوسائل التي يستخدمها مرتكب الجريمة من حيث اعتماده على الوسائل المعلوماتية الحديثة، كما أن مرتكب جرائم أمن الدولة المعلوماتي يوصف بأنه من طافة المجرمين من ذوي الخبرة الكبيرة في التقنيات الحديثة.

ومن أبرز توصيات البحث :يوصى الباحث المشرع الإتحادى الإماراتي إضافة مواد قانونية لقانون الإجراءات الجزائية الاتحادي الصادر بمرسوم بقانون اتحادي رقم (٣٨) لسنة ٢٠٢٢ تنظم تكوين نيابة أمن الدولة، والنيابة الاتحادية لمكافحة جرائم الشائعات والجرائم الإلكترونية، في الفصل الخاص بتنظيم عمل النيابة العامة.

الكلمات الدالة: أمن الدولة – أمن الدولة المعلوماتي – التحقيق- النيابة العامة – نيابة امن الدولة- التحديات التقنية- الدليل المعلوماتي.

ABSTRACT

The research aims to clarify the specificity of the investigation of state security crimes by clarifying the definition of investigation into these crimes, the competent authority for investigating state security crimes in the United Arab Emirates, and the challenges facing the investigation of these crimes.

The importance of the research from a scientific point of view is that one of the first specialized research that deals with a very important topic is the specificity of investigating state security information crimes, especially since the UAE legislator has introduced a special law to combat cybercrime, Federal Decree-Law No. (34) of 2021 on combating rumors and cybercrime, which included provisions for investigating this type of crime, and devoted special articles to criminalize and punish crimes targeting state information security, and therefore the research is considered A key pillar in dealing with a specific part in combating state security crimes, which is the investigation, because the investigation is of great importance in clarifying evidence and attributing the crime to the perpetrator

Due to the danger posed by state security crimes to society and security, the problem of the study is two-dimensional, the first dimension is the multiplicity of competent authorities in investigating state security information crimes, between the State Security Prosecution and the Federal Prosecution for rumors and electronic crimes, and this multiplicity of jurisdiction has many negative effects in investigating crimes affecting state information security, while the second dimension of the problem is the difficulties facing the investigation authority in state security crimes Information in terms of the speed of obliterating the features of the crime and the difficulty of knowing the perpetrator, and the spatial dimension of the commission of the crime, and therefore the research problem can be crystallized in the following question: What is the adequacy of the UAE procedural legislation in taking note of the privacy of state security crimes information?

Among the most prominent results of the research: The investigation of state security information crimes has a peculiarity that distinguishes it from the traditional investigation, and acquires this privacy in terms of the nature of the information state security crimes stipulated by the UAE legislator in Federal Decree-Law No. (34) of 2021 regarding combating rumors and cybercrime, and the specificity of the investigation of state security information crimes appears through the nature of the means used by the perpetrator of the crime in terms of his reliance on modern information means, and the perpetrator Cybercrime State Security is described as a group of criminals with great experience in modern technologies.

Among the most prominent recommendations of the research: The researcher wishes the UAE legislator to add legal articles to the Federal Code of Criminal Procedure promulgated by Federal Decree-Law No. (38) of 2022 regulating the formation of the State Security Prosecution and the Federal Prosecution for Combating Rumors and Cybercrimes, in the chapter on organizing the work of the Public Prosecution.

Keywords: State Security – State Information Security – Investigation – Public Prosecution – State Security Prosecution – Technical Challenges – Information Guide.

مقدمة

تعد الجرائم الماسة بأمن الدولة سواء تلك التي تمس أمن الدولة من الداخل أم من الخرج من أخطر الجرائم ،والتي يهدف مقترفوها إلى هدر القيم الأدبية والمادية للدولة .

ومن الواضح أن أولى الجرائم التي ظهرت في تاريخ التشريعات الجنائية كانت جرائم موجهة ضد المصالح العامة للجماعات وكان يعاقب عليها بعقوبة شديدة ،بينما الجرائم المرتكبة ضد الأفراد وكانت خلافاً لذلك تعد جرائم مألوفة بين المجرم والمعتدى عليه ،لذلك عاقبت التشريعات الجنائية الوضعية ،والعرفية على الجرائم التي ترتكب ضد المجموع بعقوبات يغلب عليها طابع القسوة الواضحة .

كما إن القضايا الخطرة كانت تلحق ضرراً بالمصالح العامة ،وهى جرائم فى معظمها تكون عقوبتها الإعدام ،أو النفي ،فبقدر ما كانت المجموعات البشرية تهتم بوضع قواعد واسس واضحة للتنظيم في جميع المجالات فإنها ،وبالمقابل اهتمت بوضع عقوبات قاسية لمن يخل بقواعد هذا التنظيم .

ومهما بلغت درجة الحضارة التي وصلت إليها تلك المجتمعات فقد بقيت العقوبات بالشدة ذاتها تجاه من يرتكب جريمة ماسة بأمن الدولة ، وفى ضوء أن إقليم الدولة ليس المكان الوحيد الذي يمارس عليه أفراد المجتمع نشاطه ،بل إنه في جميع العصور يتجاوزالأفراد حدود بلادهم ويتنقلون بين الأقاليم الأجنبية . فكل المجتمعات كانت تحاول جاهدة الحفاظ على أمنها ،وعلى حدودها من خلال تقوية شدة تماسكها وعدم السماح لأي من مواطنيها بإقامة علاقات أو صلات مع الجماعة المعادية لها.

كما كانت توقع أشد العقوبات على من فر من المعارك ،لأن في ذلك تعريض وجود الجماعة للخطر

ونظراً للتطور الكبير في التقنيات الحديثة ووسائل الاتصال، والذكاء الاصطناعي، لم تعد جرائم أمن الدولة ترتكب بطريقة تقليدية، بل أصبحت شبكة الإنترنت والوسائل المعلوماتية الحديثة

عنصراً هاماً في ارتكاب جرائم أمن الدولة، وقد تنبه المشرع الإماراتي لخطورة هذه الجرائم وأفرد لها باباً خاصة في المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ بشأن مكافحة الشائعات والجرائم الإلكترونية، الذي نظم قواعد التجريم والعقاب على هذا النوع من الجرائم، وكذلك فعل المشرع المصري في القانون رقم (١٧٥) لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات.

وتضمن القانون الإماراتي إضافة لقواعد التجريم والعقاب بعض المواد الخاصة بالتحقيق في الجرائم الإلكترونية التي تندرج ضمنه جرائم أمن الدولة المعلوماتي، وكذلك فعل المشرع المصري، ونظراً لأهمية هذا الموضوع وخطورة جرائم الاعتداء على أمن الدولة المعلوماتي، فإن إجراءات التحقيق فيها لها خصوصية تتميز بها عن التحقيق في بقية الجرائم الأخرى من حيث جهة الاختصاص بالتحقيق وإجراءات التحقيق وهناك العديد من المعوقات التي تطال التحقيق في جرائم امن الدولة المعلوماتي، وهو ما يعالجه البحث.

أهمية البحث

١) **الأهمية النظرية**: تتمثل أهمية البحث من الناحية النظرية في أنه يبين الإطار النظري لخصوصية التحقيق في جرائم أمن الدولة المعلوماتي، من خلال تعريف التحقيق في جرائم أمن الدولة المعلوماتي، وبيان خصائصه ومعوقاته، كما أن الدراسة تبين الإطار النظري للاختصاص في التحقيق في جرائم امن الدولة المعلوماتي، ويسهم البحث من الناحية النظرية في بيان التصور النظري للتحقيق في جرائم امن الدولة المعلوماتي.

٢) **الأهمية العلمية:** تتمثل أهمية البحث من الناحية العلمية في أنه من أوائل البحوث المتخصصة التي تتناول موضوعاً في غاية الأهمية هو خصوصية التحقيق في جرائم أمن الدولة المعلوماتي، وخاصة ان المشرع الإماراتي استحدث قانونا خاصا بمكافحة الجرائم الإلكترونية، هو المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ بشأن مكافحة الشائعات والجرائم الإلكترونية، الذي تضمن نصوصاً خاصة بالتحقيق في هذا النوع من الجرائم، وأفرد مواد خاصة للتجريم والعقاب على الجرائم التي تستهدف أمن الدولة المعلوماتي.

وعليه فإن البحث يعتبر ركيزة أساسية في تناوله لجزئية محددة في مكافحة جرائم امن الدولة المعلوماتي، وهو التحقيق، وذلك لما للتحقيق من أهمية كبيرة في استجلاء الأدلة وإسناد الجريمة لمرتكبها، وكذلك فإن البحث من الناحية العلمية يتناول موقف المشرع الإماراتي من الاختصاص في

التحقيق في جرائم أمن الدولة المعلوماتي، ويبين أوجه الاتفاق وأوجه الاختلاف في موضـوع البحث بين القوانين في دولة الإمارات العربية المتحدة وجمهورية مصـر العربية ، كما أن البحث سـيقدم بعض التوصـيات التي تسـهم في سـد الثغرات وتوضـيح بعض القواعد الخاصـة بالتحقيق في الجرائم الإلكتروني التي تستهدف امن الدولة المعلوماتي، الامر الذي يمكن الاستفادة منه مستقبلاً في تطوير التشريعات الإجرائية في دولة الإمارات العربية المتحدة وجمهورية مصر العربية.

مشكلة البحث:

نظراً لما تشكله جرائم أمن الدولة المعلوماتي من خطر على المجتمع والامن، فإن مشكلة الدراسة تكون ذات بعدين، البعد الأول هو تعدد جهات الاختصـاص في التحقيق في جرائم أمن الدولة المعلوماتي، بين نيابة أمن الدولة وبين النيابة الاتحادية لجرائم الشائعات والجرائم الإلكترونية، وهذا التعدد في الاختصاص له العديد من الآثار السلبية في التحقيق في الجرائم التي تمس أمن الدولة المعلوماتي.

أما البعد الثاني من المشـكلة هو الصـعوبات التي تواجه جهة التحقيق في جرائم امن الدولة المعلوماتي من حيث سـرعة طمس معالم الجريمة وصـعوبة معرفة مرتكبها، والبعد المكاني لارتكاب الجريمة، وعليه يمكن بلورة مشكلة البحث في التساؤل التالي: ما مدى كفاية التشريعات الإجرائية الإماراتية في الإحاطة بخصوصية جرائم امن الدولة المعلوماتي؟

أسئلة البحث:

١) ما هو امن الدولة المعلوماتي؟ وما يميزه عن أمن الدولة التقليدي؟
٢) ما هي خطورة جرائم امن الدولة المعلوماتي على المجتمع والامن؟
٣) من هي الجهة المختصة بالتحقيق في جرائم امن الدولة المعلوماتي؟
٤) ما هي الإجراءات الخاصة بالتحقيق في جرائم امن الدولة المعلوماتي؟
٥) ما هي أبرز الصعوبات والعقبات التي تعترض جهة التحقيق في جرائم أمن الدولة المعلوماتي؟
٦) ما مدى كفاية القواعد القانونية الإجرائية للإحاطة بالإجراءات الخاصـة بالتحقيق بأمن الدولة المعلوماتي؟

أهداف البحث

١) الإحاطة بماهية التحقيق في جرائم أمن الدولة المعلوماتي؟
٢) تحديد الجهة المختصة بالتحقيق في جرائم أمن الدولة المعلوماتي في دولة الإمارات العربية المتحدة ؟
٣) إبراز الصعوبات والتحديات التي تواجه جهة التحقيقي في جرائم أمن الدولة المعلوماتي؟
٤) بيان إجراءات التحقيق في جرائم امن الدولة المعلوماتي؟

نطاق البحث

١) النطاق المكاني: دولة الإمارات العربية المتحدة.
٢) النطاق الزمني: منذ عام ٢٠١٨ إلى عام ٢٠٢٣.
٣) النطاق الموضوعي: خصوصية التحقيق في جرائم أمن الدولة المعلوماتي.

منهج البحث

يعتمد البحث على المنهج الوصفي التحليلي والمنهج المقارن، وذلك من خلال وصف الموضوع من الناحية النظرية من حيث المفهوم والخصائص، وتحليل الآراء الفقهية والمواد القانونية الواردة في التشريعات الإماراتية وأحام القضاء المرتبطة بموضوع البحث، ومقارنة التنظيم القانوني للتحقيق في جرائم أمن الدولة المعلوماتي في دولة الإمارات العربية المتحدة مع ما هو معمول به في الدولة.

الدراسات السابقة

دراسة بعنوان **:" الجرائم الواقعة على أمن الدولة الداخلي باستخدام شبكة الإنترنت"**[1]حيث بينت الدراسة: ان هناك العديد من صور الجرائم الماسة بأمن الدولة من جهة الخارج، حيث تأخذ تلك الجرائم صورة السعي أو التخابر لدى دولة أجنبية أو لدى من يمثلها، كما تعتبر جريمة ‘فشاء أسرار الدفاع باستخدام التقنيات الحديثة من صور جريمة المساس بأمن الدولة من جهة الخارج، وجريمة إذاعة الأخبار الكاذبة أثناء الحرب باستخدام التقنيات الحديثة، وجريمة تسليم معلومات خاصة بالدولة باستخدام التقنيات الحديثة، وتعتبر وسائل تقنية المعلومات هي الوسيلة المستخدمة بارتكاب الجرائم الماسة بأمن الدولة من جهة الخارج، ولابد لنا من التعرف

[1] حسن البلوشي: الجرائم الواقعة على أمن الدولة الداخلي باستخدام شبكة الإنترنت، رسالة ماجستير، أكاديمية شرطة دبي، دبي، ٢٠١٧

على ماهية نظم التقنيات الحديثة المستخدمة في ارتكاب الجرائم الماسة بأمن الدولة من جهة الخارج، عن طريق تعريفها وأساليب استخدامها، كما تعتبر الجرائم الماسة بأمن الدولة من جهة الخارج من أخطر الجرائم على الإطلاق وذلك لما تنطوي عليه هذه الجرائم من تهديد للمجتمع بكل أطيافه، وخاصة تلك التي يتم ارتكابها بواسطة التقنيات الحديثة التي تعمل عن طريق شبكة الإنترنت حيث تستغل الجماعات الإرهابية المتطرفة الفضاء الإلكتروني كوسيلة لارتكاب جرائمها الماسة بأمن الدولة من جهة الخارج، وخاصة وسائل تقنيات المعلومات الحديثة لما تحتويه من تطبيقات وبرامج تعمل على الأجهزة الذكية المتطورة والتي تجمع بين خصائص الحاسب الآلي ووسائل الاتصال الحديثة التي تعمل على شبكة المعلومات الدولية (الإنترنت)، ومن أبرز صور الجرائم الماسة بأمن الدولة من جهة الخارج والتي تستخدم فيها التقنيات الحديثة جريمة التخابر لدى دولة أجنبية، والتي يتم فيها استخدام الوسائل الحديثة للتواصل بين أفراد الجماعات الإرهابية المتطرفة بعيداً عن أعين رجال الأمن، ويسعى المجرمون في سبيل الإضرار بأمن الدولة من جهة الخارج لاستخدام وسائل متطورة أكثر خطورة تعمل بواسطة الإنترنت وخاصة تلك التي تعمل بوسائل اتصال المشفرة التي يصعب تعقبها ورصد أفرادها.

ما يميز البحث عن الدراسة السابقة: إن البحث يتناول التحقيق في جرائم امن الدولة المعلوماتي بينما الدراسة السابقة تناولت فقط جرائم امن الدولة الداخلي من الناحية الموضوعية دون التطرق للناحية الإجرائية.

دراسة بعنوان **: جريمة الإتلاف المعلوماتي"**[2]. يعد موضوع الجرائم الإلكترونية مع حداثته سمة العصر، فحداثته تنبع مع تعلقه بالأنشطة الإجرامية المرتكبة بوساطته أو ضد أدوات التقنية الالكترونية (الحاسب الآلي والإنترت) ، وبالتالي فإن الجرائم المرتبط بها تعد حديثة كذلك وتنبع معاصرته وأهميته من كون الأنشطة الإجرامية المتعلقة بالمعلومات تتعدد وتجدد باستمرار وفي أشكال خطيرة. وتكمن أهمية الدراسة في الحرص على مواجهة الجرائم الواقعة على المعلومات ومن أهمها جريمة الإتلاف الإلكتروني لما لها من خطورة بالغة على الدول والأفراد، وكذلك قيام الدولة بسن المزيد من القوانين المتعلقة بجريمة الإتلاف الإلكتروني من أجل وقف الأعمال الناتجة عن أعمال مشبوهة أو جرائم مالية، لأن إتلاف المعلومات يؤدي إلى نتائج كبيرة وخسائر عظيمة سواء للدولة من حيث إتلاف المعلومات المهمة والتي يؤدي إتلافها إلى وقوع ضرر على الدولة وعلى الجانب الآخر إتلاف المعلومات للأفراد قد يؤدي إلى حدوث خسائر فادحة لهم. تكمن مشكلة الدراسة في أن التشريعات المتخصصة بجرائم تقنية المعلومات والتي سبق ذكرها في مقدمة الدراسة لم

[2]ياسر الكتبي: جريمة الإتلاف الإلكتروني في قوانين دول مجلس التعاون لدول الخليج العربية أطروحة ماجستير لاستكمال متطلبات الحصول على درجة الماجستير في القانون العام، جامعة عجمان، ٢٠٢٣.

تتعرض لتعريف جريمة الإتلاف في صورتها الإلكترونية مكتفية بإيراد صور السلوك الإجرامي الذي تتحقق به هذه الجريمة. فنلاحظ في القانون البحريني والقطري التداخل بين جريمة الإتلاف الإلكتروني وجريمة إعاقة النظام الإلكتروني. ومن أبرز نتائجها ان جريمة الإتلاف هي نتيجة لجريمة تكون سابقة لها هي جريمة الاختراق الإلكتروني والبقاء غير المشروع في المواقع الإلكترونية بهدف الإتلاف. ومن أبرز توصياتها: يوصي الباحث بأن يقوم المشرع الإماراتي بإفراد فصل خاص ضمن المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ بحيث يكون تحت عنوان (جريمة الاتلاف وما يرتبط بها من جرائم) حيث أن موضوع جريمة الإتلاف لم يذكر إلا في المادة الثانية والثالثة من القانون الإماراتي كأحد نتائج الاختراق.

وما يميز البحث عن الدراسة السابقة أنها يتناول التحقيق في الإتلاف المعلوماتي كأحد أنواع جرائم الاعتداء على أمن الدولة المعلوماتي، ولكن الدراسة السابقة تناولت الإتلاف من الجانب الموضوعي دون التطرق للجانب الإجرائي.

تقسيم البحث

المبحث الأول: ماهية التحقيق في جرائم أمن الدولة المعلوماتي

- المطلب الأول: تعريف التحقيق في جرائم أمن الدولة المعلوماتي.
- المطلب الثاني: السمات الخاصة بالتحقيق في جرائم أمن الدولة المعلوماتي.

المبحث الثاني: الجهة المختصة بالتحقيق في جرائم أمن الدولة المعلوماتي

- المطلب الأول: نيابة أمن الدولة
- المطلب الثاني: النيابة الاتحادية لجرائم الشائعات والجرائم الإلكترونية

المبحث الثالث: تحديات التحقيق في جرائم أمن الدولة المعلوماتي

- المطلب الأول: طبيعة مرتكبي جرائم أمن الدولة المعلوماتي
- المطلب الثاني: طبيعة الوسائل المستخدمة في ارتكاب جرائم أمن الدولة المعلوماتي
- المطلب الثالث: التحديات المرتبطة بالدليل الخاص بالجريمة
- **الخاتمة**
- **النتائج**
- **التوصيات**

- **قائمة المراجع**

المبحث الأول

ماهية التحقيق في جرائم أمن الدولة المعلوماتي

أفرزت الثورة المعلوماتية الحديثة نوعاً جديداً من الجرائم وهو ما يسمى بالجرائم الرقمية أو الجرائم المعلوماتية والتي تمثل أنماطاً متعددة من السلوك الإجرامي تتم من خلال الأجهزة الحاسوبية والشبكة المعلوماتية، وحيث إن الجريمة الرقمية ترتكب في عالم افتراضي فقد أُثير التساؤل حول مدى تطور إجراءات التحقيق الجنائي حتى يمكن التعامل مع هذا النوع الجديد من الإجرام حيث إنها تخضع بالضرورة لإجراءات تختلف عن القواعد الإجرائية التقليدية لاستخلاص الدليل الجنائي، ولذلك كانت أهمية موضوع البحث وهو التحقيق الجنائي الرقمي القائم على التحليل الجنائي الرقمي باستخدام التقنيات التكنولوجية الحديثة، للحصول على ما يسمى بالدليل الرقمي وتحقيقه بالطرق المثبتة علمياً والتي تؤكد على ضرورة مشروعيته.

ولذلك ارتكز هذا البحث على معرفة الأصول القانونية للتحقيق الجنائي الرقمي من خلال بيان أصول وقواعد هذا التحقيق وما يعترضه من معوقات، وكذلك معرفة الآليات الإجرائية الحديثة لاستخراج الأدلة الرقمية من أجهزة الحاسب الآلي والشبكة المعلوماتية، وتم اتباع المنهج التحليلي في بيان قواعد وإجراءات هذا التحقيق[3].

وجرائم أمن الدولة المعلوماتي من الجرائم التي نظم المشرع الإماراتي قواعد التجريم والعقاب فيها في مرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ بشأن الشائعات والجرائم الإلكترونية، وإننا في البحث لسنا بصدد البحث في قواعد التجريم والعقاب، بل البحث في التحقيق في هذه الجرائم من حيث تعريف التحقيق والجهة المختصة به، وعليه نتناول في هذا المبحث ماهية التحقيق في جرائم أمن الدولة المعلوماتي، من خلال مطلبين على النحو التالي:

- المطلب الأول: تعريف التحقيق في جرائم أمن الدولة المعلوماتي.
- المطلب الثاني: السمات الخاصة بالتحقيق في جرائم أمن الدولة المعلوماتي.

---

[3] حنان محمد الحسيني أحمد، وسحر علي عبدالله الهبدان. "التحقيق الجنائي الرقمي". مجلة جامعة الملك سعود - الحقوق والعلوم السياسية مج ٣٣، ع٢، (٢٠٢١): ١٢ص٩ -.

المطلب الأول

تعريف التحقيق في جرائم أمن الدولة المعلوماتي

المطلع على قانون الإجراءات الجزائية لدولة الإمارات العربية المتحدة رقم ٣٨ لسنة ٢٠٢٢ ، يلحظ تأثره بالنظام الإجرائي المختلط والنظام الإجرائي الإسلامي، مع الاحتفاظ ببعض الملامح الخاصة، التي يقتضيها التطور خصوصا في المجال التقني واستغلال المشرع لذلك لتبسيط الإجراءات من أجل السرعة في الانجاز كما سنشير لاحقاً. فقد قسم المشرع الإماراتي الدعوى الجزائية إلى مرحلتين: مرحلة التحقيق الابتدائي، ومرحلة المحاكمة ، ويغلب على مرحلة التحقيق الابتدائي طابع نظام التنقيب والتحري[4].

ونظراً لأهمية مرحلة التحقيق في جرائم أمن الدولة المعلوماتي، نبين في هذا المطلب تعريف التحقيق لغةً واصطلاحاً وفي الفقه القانوني وفي التشريعات على النحو التالي:

أولاً: تعريف التحقيق لغةً

عرفه بن المنظور[5] بأنه "التصديق أو التأكيد أو التثبيت تقول حقق فلان ظنه بمعنى صدقه وحقق الأمر أي أكده وثبته "، كما عرفه الجبالي أيضا[3] بأنه "حقق الأمر أي أثبته وصدقه بمعنى حقق مع فلان في قضية وأخذ أقواله فيها ويتعدد المقصود اللغوي طبقاً لمجالات استخدامها". كما يعرف أيضا: على انه "الحق ضد الباطل والحق: العدل، وحقق الأمر: ثبت ووقع بلا شك"[6]

---

[4]الدكتور محمد شلال العاني و الاستاذ الدكتور عبدالإله محمد النوايسة: شرح قانون الإجراءات الجزائية الإماراتي في ضوء المرسوم بقانون اتحادي رقم (٣٨) لسنة ٢٠٢٢ ، دار النهضة العربية، القاهرة، ٢٠٢٣، ص ٢١

[5] - ابن المنظور، أبو الفضل جمال الدين، **"لسان العرب "**، المجلد الأول، دار صادر للطباعة والنشر، بيروت ٢٠٠٠ ، ص ٢٤.

[3] - الجبالي منصور بن عبد العزيز، "مبادئ التحقيق الجنائي"، مكتبة فهد الوطنية، الطبعة الأولى ٢٠٠٨، ص ٦٠.

[6]د. محمود سليمان موسى: الجرائم الواقعة على أمن الدولة، دار المطبوعات الجامعية، الإسكندرية، ٢٠٠٩م، ص ٣.

ثانياً: تعريف التحقيق في الاصطلاح القانوني

عرفه جانب من الفقه بأنه مجموعة من الإجراءات القضائية تمارسها سلطات التحقيق بالشكل المحدد قانوناً بغية التنقيب عن الأدلة في شأن جريمة ارتكبت وتجميعها ثم تقديرها لتحديد مدى كفايتها في إحالة المتهم إلى المحاكمة، أو الأمر بألا وجه لإقامة الدعوى[7] وعرفه جانب آخر من الفقه بأنه عبارة عن سلسلة من الإجراءات التي تتخذها السلطات المختصة بهدف التنقيب عن الأدلة في شأن الجريمة المرتكبة لتحديد مدى كفايتها لإحالة المتهم إلى المحكمة المختصة[8].

ويعرف أيضاً، "بأنه الجهد المبذول لكشف غموض الجرائم وتحديد شخصية مرتكبيها وإثبات التهمة عليهم بما يقدم من أدلة إثبات وهو العلم الذي يوضح الوسائل الفنية التي على هداها يمارس العاملون في حقل مكافحة الجريمة وضبطها وتحقيقها اختصاصاتهم التي خولها لهم القانون عند وقوع الجريمة وتصديهم لمواجهتها"[9].

كما يعرف بانه:" بأنه تحقيقاً ابتدائياً شاملاً لجميع الإجراءات التي يباشرها المحقق عند وقوع جريمة أو حادث توصلاً إلى معرفة الحقيقة ولكن فيما يسمى بالجرائم الرقمية؛ فهو ينطوي على عملية الفحص والتدقيق لأي جهاز كمبيوتر أو أي جهاز ملحق به لتحديد ما إذا كان هذا الجهاز قد تم استخدامه في جريمة رقمية أو عمل غير مشروع ثم تحقيق الأدلة الخاصة بذلك"[10].

وقد عرفه البعض بأنه :"كافة الجهود التي يبذلها فريق التحقيق في سبيل استنطاق الأدلة الرقمية لكشف غموض جرائم الحاسوب والإنترنت وتحديد شخصية مرتكبها وإثباتها بما يقدمه من أدلة إثبات"[11]

---

[7] د. أمير فرج يوسف: جرائم أمن الدولة العليا في الداخل والخارج، دار المطبوعات الجامعية، الإسكندرية، ٢٠٠٩م، ص٩.

[8] سمير عالية: الوجيز في شرح الجرائم الواقعة على أمن الدولة، المؤسسة الجامعية للدراسات والنشر والتوزيع، ط١، بيروت، ١٩٩٩م، ص ٤٩.

[9] - عبد الله بن حسين الجراف القحطاني، **"تطوير مهارات التحقيق الجنائي في مواجهة الجريمة المعلوماتية "**، رسالة مقدمة لنيل شهادة الماجستير، قسم العلوم الشرطية، جامعة نايف للعلوم الأمنية، الرياض ٢٠١٤، ص١٢-١٣.

[10] د. أيمن ناصر بن حمد العباد: المسؤولية الجنائية لمستخدمي شبكات التواصل الاجتماعي، مكتبة القانون والاقتصاد، الرياض، ط١، ٢٠١٦م، ص ٧٠.

[11] د. ضرغام جابر عطوش آل مواش: جريمة التجسس المعلوماتي، المركز العربي للنشر، مكتبة دار السلام القانونية، القاهرة، ٢٠١٦، ص ٢٩.

وتنـاط هـذه المرحلـة بالنيابـة العامـة التـي تعـد شـعبة مـن شـعب السـلطة القضـائية، وهـي جهـاز رسـمي، ويـتم التحقيـق بشـكل سـري ولا يسـمح لغيـر الأطـراف والأشـخاص المعنيـين بالحضـور، كمـا أن جميـع الإجـراءات يـتم تـدوينها ، ولا يجـوز اللجـوء للتعـذيب لحمـل المـتهم علـى الاعتـراف والتحقيـق الجنـائي الرقمـي يحمـل ذات المضـمون السـابق ويعتبـر تحقيقـاً ابتـدائياً موضـوعه تحقيـق الأدلـة الرقميـة ولكـن بصفة خاصة في الجرائم الرقمية.

ومـن خـلال مـا سـبق مـن تعريفـات للتحقيـق يعـرف الباحـث التحقيـق فـي جـرائم أمـن الدولـة المعلومـاتي بأنـه:" الجهـود التـي تقـوم بهـا النيابـة العامـة الاتحاديـة لجـرائم الشـائعات والجـرائم الإلكترونيـة لكشـف غمـوض الجـرائم التـي تقـع علـى أمـن الدولـة باسـتخدام التقنيـات الحديثـة، أي الجـرائم التـي تمـس أمـن الدولـة باسـتخدام الأنظمـة المعلوماتيـة، بهـدف كشـف غمـوض الجـرائم والوصـول لمرتكـب جـرائم أمـن الدولة المعلوماتي، والحصول على الأدلة التي تثبت إدانة مرتكب الجريمة".

ثالثاً: التعريف التشريعي للتحقيق

تعـد مرحلـة الاسـتدلال والتحـري مرحلـة تمهيديـة لمرحلـة التحقيـق الابتـدائي ويتـولى القيـام بهـذه المرحلـة مـأمورو الضـبط القضـائي، ويـتم خـلال هـذه المرحلـة الأوليـة جمـع المعلومـات حـول الجريمـة المرتكبـة وجمـع الأدلـة حولهـا والكشـف عـن شـخص مرتكبهـا إذا كـان مجهـولاً مـن خـلال أسـاليب قانونية حددها المشرع [12].

وقـد نظـم المشـرع الإمـاراتي هـذه المرحلـة فـي الكتـاب الأول مـن قـانون الإجـراءات الجزائيـة فـي المـواد مـن ٣١ -٦٥ وعنونـه بـ (استقصـاء الجـرائم وجمـع الأدلـة وتحقيقهـا) ورسـمت المـادة ٣١ الإطـار العـام لإجـراءات هـذه المرحلـة ووظيفتهـا الأساسـية حيـث نصـت علـى أنـه : (يقـوم مـأمورو الضـبط القضـائي بتقصـي الجـرائم والبحـث عـن مرتكبيهـا وجمـع المعلومـات والأدلـة اللازمـة للتحقيـق والاتهام)

[12] عرفـت المـادة ٥١ مـن التعليمـات القضـائية للنيابـة العامـة فـي دولـة الإمـارات العربيـة المتحـدة لسـنة ٢٠٠٧ مرحلـة الاسـتدلال بأنهـا : (الاسـتدلال هـو المرحلـة السـابقة علـى تحريـك الـدعوى الجزائيـة ويباشـره رجـال الشـرطة مـن ذوي الاختصـاص العـام فـي الضـبط القضـائي بـدوائر اختصاصـهم وغيـرهم ممـن لهـم صـفة الضـبطية القضـائية فـي نطـاق معين، كمفتشي الصحة والعمل والشئون الاجتماعية والبلديات).

من خلال النص السابق يتضح لنا الفرق بين هذه المرحلة الأولية وبين مرحلة التحقيق الابتدائي حيث أن إجراءات الاستدلال تباشر خارج إطار الدعوى الجزائية ولا تعتبر إجراءاتها من إجراءات التحقيق، فهي مرحلة تمهيدية لمرحلة التحقيق الابتدائي فهي مجرد تقصي عن الجرائم وجمع أدلتها دون تنقيب فيها ودون فحصها، ولا تتضمن حجز أو قيد على حرية المشتبه بهم إلا في حالات استثنائية نص عليها قانون الإجراءات الجزائية الاتحادي[13]

وتباشر إجراءات مرحلة الاستدلال والتحري من قبل مأموري الضبط القضائي تحت إشراف النيابة العامة، بينما تتولى النيابة التحقيق الابتدائي كجهة أصيلة ولا يقدح من ذلك اختصاص مأموري الضبط القضائي ببعض إجراءات التحقيق الابتدائي في حالات استثنائية ولا يحول وجود قيود على حرية النيابة العامة في تحريك دعوى الحق العام كقيد الشكوى والطلب والإذن دون مباشرة إجراءات الاستدلال، بينما تعتبر هذه القيود عقبة إجرائية لا يجوز اتخاذ إجراءات التحقيق الابتدائي إلا إذا تم تقديم شكوى أو طلب أو تم أخذ الاذن في الملاحقة[14]

وتنقطع المدة التي تنقضي بها الدعوى الجزائية بإجراءات التحقيق دون قيد أو شرط ولا تنقطع هذه المدة بإجراءات الاستدلال إلا إذا اتخذت في مواجهة المتهم أو أخطر بها بشكل رسمي[15]

---

[13] د. جوده حسين جهاد : شرح قانون الإجراءات الجزائية الاتحادي، أكاديمية شرطة دبي، دبي، ، ص ٢٤١

[14] د. محمود نجيب حسني: الإجراءات الجزائية، دار النهضة العربية، القاهرة، ١٩٩٩، ص ٥٠٠.

[15] انظر المادة ٢٢ من قانون الإجراءات الجزائية الاتحادي. جاء في حكم للمحكمة الاتحادية العليا : (أن من المقرر قانوناً وفق ما نصت عليه المادة (٢١) من قانون الإجراءات الجزائية الاتحادي، وما استقر عليه الضاء هذه المحكمة أن تقادم الدعوى الجزائية ينقطع بإجراءات التحقيق أو الاتهام أو المحاكمة، وكذلك بإجراءات الاستدلال إذا اتخذت في مواجهة المتهم أو إذا أخطر بها يوجه رسمي. وأنه إذا تعددت الإجراءات التي تقطع سريان المدة، فإن سريان المدة يبدأ من تاريخ آخر إجراء صحيح، وإذا تعدد المتهمون فإن انقطاع المدة بالنسبة لأحدهم يترتب عليه انقطاعها بالنسبة للباقين». المحكمة الاتحادية العليا - الأحكام الجزائية - الطعن رقم ٢٣٩ -لسنة ٢٠١٣ قضائية - تاريخ الجلسة ٢٠١٣-١١-١٢

المطلب الثاني

السمات الخاصة بالتحقيق في جرائم أمن الدولة المعلوماتي

قسم المشرع الإماراتي الدعوى الجزائية إلى مرحلتين: مرحلة التحقيق الابتدائي، ومرحلة المحاكمة ، ويغلب على مرحلة التحقيق الابتدائي طابع نظام التنقيب والتحري فتناط هذه المرحلة بالنيابة العامة التي تعد شعبة من شعب السلطة القضائية، وهي جهاز رسمي، ويتم التحقيق بشكل سري ولا يسمح لغير الأطراف والأشخاص المعنيين بالحضور، كما أن جميع الإجراءات يتم تدوينها ، ولا يجوز اللجوء للتعذيب لحمل المتهم على الاعتراف ويغلب على إجراءات المحاكمة ملامح النظام الاتهامي، فالمحاكمة تكون علنية ومن حق الجمهور حضورها ضمن ضوابط معينة، ونستطيع القول: إنَّ الأطراف لهم حقوق متماثلة، وتتم الإجراءات والمرافعات بشكل شفوي وإن تم تدوينها في محاضر، وللمتهم الاستعانة بمحام للدفاع عنه[16].

لقد اتجهت التشريعات الوضعية إلى وضع قواعد إجرائية خاصة ومستقلة عن الجرائم العادية، وذلك بما يؤدي إلى التوسع في سلطات الجهات القائمة على ضبط هذه الجرائم وتعقبها، وعلى هذا فإن الجرائم الماسة بأمن الدولة الداخلي وجرائم الإرهاب تقرر صلاحيات واسعة لسلطات الضبط والتحقيق والاتهام والمحاكمة، ويرجع خروج هذه الجرائم عن القواعد العامة في الإجراءات الجنائية إلى خطورة مرتكبي هذه الجرائم واتصالهم بتنظيمات إرهابية قد تساعدهم على طمس الأدلة وسرعة الهروب من العدالة داخل البلاد أو خارجها[17].

ولكن مما يجب أن نشير إليه أن هذه الإجراءات الخاصة يجب أن تكون بالقدر الضروري الذي يتلاءم مع الهدف منها، ومع مراعاة حدود التناسب بين اعتبارات الأمن وحقوق الإنسان، وهذا ما يقتضي منا الحديث عن القواعد الإجرائية لمكافحة جرائم الإرهاب نبدأها بالتشريع المصري، وذلك في مراحلها المختلفة ثم نقوم بإلقاء الضوء على القواعد الإجرائية الخاصة بالإرهاب في

---

[16] الدكتور محمد شلال العاني و الاستاذ الدكتور عبدالإله محمد النوايسة: شرح قانون الإجراءات الجزائية الإماراتي في ضوء المرسوم بقانون اتحادي رقم (٣٨) لسنة ٢٠٢٢ ، دار النهضة العربية، القاهرة، ٢٠٢٣، ص٢١.

[17] السويدي، أحمد غانم سيف (٢٠١٦). المواجهة الجنائية والأمنية للجرائم الماسة بأمن الدولة الداخلي دبي: أكاديمية شرطة دبي، كلية الدراسات العليا.

بعض التشريعات الأجنبية والعربية، ونعقب على ذلك بموقف الشريعة الإسلامية من القواعد الإجرائية الخاصة بالجرائم الإرهابية[18].

يتم تسجيل وحفظ الإجراءات عن بعد إلكترونيا ويكون لها صفة السرية ولا يجوز تداولها أو الإطلاع عليها أو نسخها من النظام المعلوماتي إلا بإذن من النيابة العامة أو المحكمة المختصة [19] ، ويجوز للجهة المختصة تفريغ الإجراءات عن بعد في محاضر أو مستندات ورقية أو إلكترونية تعتمد منها دون حاجة لتوقيع من أصحاب العلاقة[20]

كما ان المشرع الإماراتي نص على جواز استخدام الإجراءات عن بعد مع الدول الأجنبية أجازت المادة ٤٢٣ من قانون الإجراءات الجزائية استخدام الإجراءات عن بعد في تنفيذ الانابات والمساعدات القضائية مع الدول الأجنبية وفقاً لأحكام الاتفاقات والمعاهدات المبرمة مع هذه الدول. وهذا الأمر من شأنه تسهيل الإجراءات الجزائية التي تتم خارج إقليم الدولة .

ومما سبق يرى الباحث ان أبرز سمات التحقيق في جرائم امن الدولة المعلوماتي هو السرية في التحقيق، نظراً لتوعية هذه الجرائم وخطورتها على المجتمع كون سرية التحقيق تسهم بشكل كبير في عدم تسريب التحقيق وإمكانية هروب او تواري مرتكب الجريمة او الشركاء فيها.

---

[18] محمد مراد عبد الله: شبكات التواصل الاجتماعي ودورها في نشر الأفكار الهدامة، بحوث ودراسات شرطية، مركز دعم اتخاذ القرار، شرطة دبي، العدد (٢٦٤) ديسمبر ٢٠١٣، ص ٤.

[19] المادة ٤٢٠ من قانون الإجراءات الجزائية.

[20] المادة ٤٢٢ من قانون الإجراءات الجزائية.

المبحث الثاني

الجهة المختصة بالتحقيق في جرائم أمن الدولة المعلوماتي

نتناول في هذا المبحث الجهة المختصة بالتحقيق في جرائم أمن الدولة المعلوماتي من خلال مطلبين على النحو التالي:

- المطلب الأول: نيابة أمن الدولة
- المطلب الثاني: النيابة الاتحادية لجرائم الشائعات والجرائم الإلكترونية

المطلب الأول

نيابة أمن الدولة

أول سؤال قانوني ينبغي طرحه عند الحديث عن التحقيق في جرائم المعلوماتية هو؛ من هو الشخص الذي يحق له جمع وتحليل الأدلة الجنائية الرقمية؟ وللإجابة على ذلك نقول: الشخص الذي يُكلف بجمع الأدلة الرقمية هو الخبير المتخصص والمدرب على معالجة جميع أنواع الأدلة الرقمية وفحصها وتحليلها. إن عمليات الضبط والحجز والتأمين وتحليل الأدلة الرقمية المخزنة في شبكات المعلوماتية هي التحدي الذي يواجه أجهزة العدالة الجنائية في هذه المرحلة التي تعاني فيها تلك الأجهزة من الأمية المعلوماتية[21].

وفي الوقت الذي تم فيه إعداد الخبراء والمختبرات الجنائية اللازمة للتعامل مع الأدلة المادية، برزت مشكلة الأدلة الرقمية كنتيجة لانتشار تقنية المعلومات في مجال الجريمة، الأمر الذي يتطلب معامل ومختبرات خاصة وإعداد خبراء يجمعون بين المعرفة القانونية ومهارة التحقيق وعلوم تقنية المعلومات. علاوةً على ذلك، يتطلب مواجهة التحدي الجديد بناء قدر من التعاون والثقة بين أجهزة تنفيذ القوانين والمؤسسات التي تقوم بتقديم خدمات المعلومات والاتصالات[22].

---

[21] د. سليمان أحمد فضل: المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الإنترنت)، دار النهضة العربية، سنة ٢٠١٣، ص ٣٩٤.

[22] Rosenblatt. K. S. High-Technology Crime: Investigating Cases Involving Computer. San Jose: KSK Publications. 1999, P. 21. 159.

ونظم المشرع الإماراتي النيابة العامة في الدولة، وجعل من ضمن تنظيمها نيابة متخصصة بجرائم أمن الدولية أطلق عليها مسمى (نيابة أمن الدولة)، وأسند لوزارة العدل تنظيم الهيكل الخاصة بجميع النيابات العامة في الدولة ومن ضمنها نيابة أمن الدولة حيث تنص المادة (٧) من قرار وزير العدل رقم ٥٥٧ لسنة ٢٠٠٩ بشأن الهيكل التنظيمي للنيابة العامة الاتحادية على انه[23]:" تقوم نيابات الدولة بتنفيذ سياسات النيابة العامة وقراراتها بما يعزز استقلاليتها والارتقاء بمستوى العمل القضائي في المناطق التي تخدمها. ويصدر النائب العام الهياكل الفرعية التي تنظم عمل نيابات الدولة حسب ما تقتضيه طبيعة عمل كل منها وهي-:

١) نيابة النقض.
٢) نيابة أمن الدولة.
٣) نيابات الاستئناف.
٤) النيابات الكلية.
٥) النيابات الجزئية.
٦) النيابات المتخصصة."

ومن هذا النص يتضح أن نيابة أمن الدولة تكون متخصصة بجرائم أمن الدولة بكافة أنواعها، حيث منح المشرع الإماراتي نيابة أمن الدولة اختصاصات قضائية وأخرى خاصة بالإجراءات الجزائية، حيث بينت المادة (٢) من ذات القرار اختصاصات النيابة العامة بالتحقيق حيث تنص على انه:" اختصاصات النيابة العامة، تختص النيابة العامة الاتحادية بما يلي[24]

١) إجراء التحقيقات القضائية.
٢) إجراء التحقيقات اللازمة سواء بفحص الأدلة المتوفرة أو سماع الشهود واستجواب المتهم ومواجهته بالأدلة القائمة ضده.

---

[23]دولة الإمارات العربية المتحدة - قرار وزير العدل - رقم ٥٥٧ لسنة ٢٠٠٩ الصادر بتاريخ ٢٠٠٩-٠٧-١٦ نشر بتاريخ ٢٠٠٩-٠٧-٣٠ يعمل به إعتبارا من ٢٠٠٩-٠٧-٣٠ بشأن الهيكل التنظيمي للنيابة العامة الاتحادية. الجريدة الرسمية ٤٩٦ السنة التاسعة والثلاثون

[24]دولة الإمارات العربية المتحدة - قرار وزير العدل - رقم ٥٥٧ لسنة ٢٠٠٩ الصادر بتاريخ ٢٠٠٩-٠٧-١٦ نشر بتاريخ ٢٠٠٩-٠٧-٣٠ يعمل به إعتبارا من ٢٠٠٩-٠٧-٣٠ بشأن الهيكل التنظيمي للنيابة العامة الاتحادية. الجريدة الرسمية ٤٩٦ السنة التاسعة والثلاثون

٣) الاستعانة بالخبراء في سبيل الوصول إلى الحقيقة وبعد أن تكتمل عناصر القضية فإن ذلك يعتبر إيذانا بالفراغ من التحقيق."

ومن هذه المادة يتضح أن المشرع الإماراتي منح نيابة أمن الدولة سلطة التحقيق في الجرائم الماسة بأمن الدولة سواء كان الداخلي او الخارجي، وقد أيدت المحكمة الاتحادية العليا اختصاص نيابة أمن الدولة في التحقيق والاستجواب في حكم لها جاء فيه:" استجوبهما رئيس نيابة أمن الدولة حيث أفاد المتهم[25]".

وفي حكم آخر للمحكمة الاتحادية العليا يؤكد دور نيابة أمن الدولة في التحقيق جاء فيه:" وشهد الرائد .... الضابط بجهاز أمن الدولة في تحقيقات النيابة العامة أن معلومات وردت للجهاز تفيد أن المتهم الأول .... بأنه جهادي وينوي القيام بعمل إرهابي داخل الدولة وعلى صلة بعناصر إرهابية أجنبية وهما"[26]

المطلب الثاني

النيابة الاتحادية لجرائم الشائعات والجرائم الإلكترونية

استحدث المشرع الإماراتي في مرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ بشان مكافحة الشائعات والجرائم الإلكترونية نيابة عامة متخصصة بجرائم أمن الدولة المعلوماتي، حيث أسند المشرع الإماراتي لوزارة العدل في دولة الإمارات العربية المتحدة تنظيم عمل النيابة الاتحادية لجرائم الشائعات والجرائم الإلكترونية، وهي تشمل اختصاصها في التحقيق في جرائم امن الدولة المعلوماتي، حيث تنص المادة الأولى من قرار وزير العدل رقم (١٣٤) لسنة ٢٠٢٢ على انه:" ينشأ بمكتب النائب العام نيابة متخصصة تسمى "النيابة الاتحادية لمكافحة الشائعات والجرائم الإلكترونية[27]".

---

[25]المحكمة الإتحادية العليا - الأحكام الجزائية - الطعن رقم ١٩٦ لسنة ٣٠ قضائية بتاريخ ٢٠٠٢-١١-٢٥ [رفض]

[26]المحكمة الإتحادية العليا - الأحكام الجزائية - الطعن رقم ١١٣ لسنة ٣٣ قضائية بتاريخ ٢٠٠٥-٠٦-٠٦ [تصحيح الحكم]

[27]دولة الإمارات العربية المتحدة - قرار وزير العدل - رقم ١٣٤ لسنة ٢٠٢٢ الصادر بتاريخ ٢٠٢٢-٠٢-١٨ نشر بتاريخ ٢٠٢٢-٠٢-٢٨ يعمل به إعتبارا من ٢٠٢٢-٠٢-١٨ بشأن إنشاء النيابة الاتحادية لمكافحة الشائعات والجرائم الإلكترونية. الجريدة الرسمية ٧٢٢ السنة الثانية والخمسون

وقد حدد قرار وزير العدل الطبيعة القانونية لهذه النيابة بأنها نيابة متخصصة في جرائم أمن الدولة المعلوماتي، وذلك وفق نص المادة (٢) منه التي تنص على أنه:" النيابة الاتحادية لمكافحة الشائعات والجرائم الإلكترونية نيابة مختصة بجرائم أمن الدولة، تتولى التحقيق والتصرف ومباشرة الدعاوى الجزائية الناشئة عن الجرائم المنصوص عليها في المواد (٣)، (٥)، (٧)، (١١) البند ٣، (١٢) البند ٣، (١٣)، (١٩)، (٢٠)، (٢١)، (٢٢)، (٢٣)، (٢٤)، (٢٥)، (٢٦)، (٢٧)، (٢٨)، (٤٧) الفقرة الثانية، (٥٢)، (٥٣)، (٥٥) من المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ في شأن مكافحة الشائعات والجرائم الالكترونية والجرائم الأخرى المرتبطة بها ارتباطا لا يقبل التجزئة[28]."

ومن خلال ما ورد في هذه المادة يتضح ان المشرع الإماراتي جعل النيابة العامة المتخصصة في هذا القرار ذات سلطة في التحقيق في جرائم امن الدولة المعلوماتي التي نص عليها مرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ بشأن مكافحة الشائعات والجرائم الإلكترونية.

وما يؤكد اختصاص هذه النيابة في التحقيق ومباشرته ما نصت عليه المادة (٣) من ذات القرار التي تنص على انه:" للنائب العام - ووفقا لما يقدره تحقيقا لاعتبارات مصلحة العمل- إحالة بعض الجرائم الواردة في المادة الثانية من هذا القرار إلى النيابات الاتحادية لمباشرة التحقيق، وفي جميع الأحوال يكون التصرف من النيابة الاتحادية لمكافحة الشائعات والجرائم الالكترونية."

ومن نص هذه المادة يتضح أن قرار وزير العدل جعل التحقيق من اختصاص هذه النيابة العامة، وذلك لخصوصية الجرائم التي تقع على أمن الدولة المعلوماتي، والتي تتطلب وجود نيابة عامة متخصصة تختلف من حيث الاختصاصات عن سلطات النيابة العامة العادية.

كما تنص المادة (٤) من ذات القرار على انه:" للنائب العام أن يحيل إلى النيابة الاتحادية لمكافحة الشائعات والجرائم الإلكترونية أي جريمة آخري وردت في المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ المشار إليه أو أي جريمة معاقب عليها بمقتضى القوانين السارية في الدولة متى ارتكبت باستخدام شبكة المعلومات أو أي نظام معلوماتي إلكتروني أو موقع إلكتروني أو وسيلة

[28]دولة الإمارات العربية المتحدة - قرار وزير العدل - رقم ١٣٤ لسنة ٢٠٢٢ الصادر بتاريخ ٢٠٢٢-٠٢-١٨ نشر بتاريخ ٢٠٢٢-٠٢-٢٨ يعمل به إعتبارا من ٢٠٢٢-٠٢-١٨ بشأن إنشاء النيابة الاتحادية لمكافحة الشائعات والجرائم الإلكترونية. الجريدة الرسمية ٧٢٢ السنة الثانية والخمسون

تقنيــة المعلومــات، والتــي تقــع فــي دوائــر الاختصــاص المكــاني للنيابــة العامــة الاتحاديــة أو دعــت مصلحة العمل إلى ذلك."

ومـن خـلال هـذه المـادة نـرى أن المشـرع الإمـاراتي لـم يجعـل الجـرائم الـواردة فـي المـادة (٢) مـن هـذا القـرار علـى إعتبارهـا جـرائم حصـرية لمباشـرة التحقيـق بهـا، بـل انـه أخـذ بعـين الاعتبـار الارتبـاط بـين جـرائم امـن الدولـة المعلومـاتي والجـرائم الأخـرى، وفـي هـذه الحالـة يـتم إحالـة الجـرائم المرتبطـة إلـى النيابة المتخصصة.

وكـذا تـنص المـادة (٥) مـن ذات القـرار علـى أنـه:" علـى النيابـات العامـة الاتحاديـة اسـتكمال مـا باشـرته مـن تحقيقـات سـابقة علـى تـاريخ صـدور هـذا القـرار وذلـك فـي الجـرائم الـواردة بالمـادة الثانيـة مـن هـذا القـرار، وإرسـالها فـور الانتهـاء منهـا بمـذكرة بـالرأي إلـى النيابـة الاتحاديـة لمكافحـة الشـائعات والجـرائم الإلكترونية للتصرف فيها.."

ومـن هـذا الـنص يتضـح ان سياسـة المشـرع الإمـاراتي فـي التحقيـق فـي جـرائم أمـن الدولـة المعلومـاتي تقـوم علـى اسـتكمال مـا كـان قائمـاً مـن تحقيقـات لـدى النيابـات العامـة فـي الدولـة فيمـا يخـص جـرائم امـن الدولــة المعلومــاتي وإرســاله إلــى النيابــة الاتحاديــة المســتحدثة بمــذكرة تتضــمن كافــة التحقيقــات حتــى تتصـرف بهـا، وهـذا يـدل علـى ان المشـرع الإمـاراتي لـم يتطلـب إعـادة التحقيـق فـي جـرائم أمـن الدولـة المعلومــاتي أمــام النيابــة الاتحاديــة لمكافحــة الشــائعات والجــرائم الإلكترونيــة، بــل تــرك لهــا التصــرف بتلـك التحقيقـات، وهنـا يؤخـذ علـى هـذه المـادة أنهـا لـم تبـين سـلطة هـذه النيابـة المتخصصـة فـي إعـادة التحقيق.

كمـا نصـت المـادة (٦) مـن ذات القـرار علـى انـه:" تتشكل النيابـة الاتحاديـة لمكافحـة الشـائعات والجـرائم الإلكترونية، من رئيس نيابة وعدد كاف من أعضاء النيابة العامة."

ومـن هـذا الـنص يتضـح أن قـرار وزيـر العـدل بـين الهيكـل التنظـيم لنيابـة أمـن الدولـة المعلومـاتي (النيابـة الاتحاديــة لجــرائم الشــائعات) حيــث أن تكوينهــا يقتصــر علــى رئــيس النيابــة وعــدد كــافي مــن أعضــاء النيابــة العامــة، ويؤخــذ علــى هــذه المــادة أن المشــرع الإمــاراتي لــم يحــدد عــدد أعضــاء النيابــة فــي هــذه النيابة المتخصصة، وترك الأمر لمقتضيات الحاجة.

ونصت المادة ٧ من ذات القرار على أنه:" يلحق بالنيابة الاتحادية لمكافحة الشائعات والجرائم الإلكترونية عدد كاف من الموظفين الإداريين والفنيين من المتخصصين ومن يرى النائب العام إلحاقه للعمل بها من العاملين بالنيابات الاتحادية والإدارات والمكاتب التابعة للنائب العام."

ومن نص هذه المادة يتضح أن وزارة العدل لم تكتفي بالنائب العام ومن يقوم مقامه في النيابة الاتحادية الخاصة بجرائم امن الدولة المعلوماتي، بل أضاف إليها كادر إداري متخصص في هذا النوع من الجرائم، وهم من أعوان القضاة من إداريين وفنيين وغيرهم، وقد احسن المشرع الإماراتي في ذلك كون جرائم أمن الدولة المعلوماتي تتطلب أساليب خاصة بالتحقيق.

كما حدد المشرع الإماراتي في نص المادة (٦٦) من مرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ بشأن الشائعات والجرائم الإلكترونية سلطات النيابة العامة في التحقيق في جرائم أمن الدولة المعلوماتي، حيث تنص على أنه[29]:"

١) في الأحوال التي تنقضي فيها الدعوى الجزائية بالتصالح أو الصلح وفقا لأحكام هذا المرسوم بقانون، للنائب العام أن يأمر بوضع المتهم تحت الإشراف أو المراقبة أو حرمانه من استخدام أي شبكة معلوماتية، أو نظام المعلومات الإلكتروني، أو أي وسيلة تقنية معلومات أخرى، أو إخضاعه لأحد برامج التأهيل للمدة التي يراها مناسبة.
٢) للنائب العام متى قامت أدلة على قيام موقع إلكتروني يبث من داخل الدولة أو خارجها، بوضع أي عبارات أو أرقام أو صور أو أفلام أو أي مواد دعائية، أو ما في حكمها بما يعد جريمة من الجرائم المنصوص عليها في المادة (٧١) من هذا المرسوم بقانون، أو يشكل تهديدا للأمن الوطني أو يعرض أمن الدولة أو اقتصادها الوطني للخطر، أن يأمر بحجب الموقع أو المواقع محل البث، كلما أمكن تحقيق ذلك فنيا أو إصدار أي من الأوامر المنصوص عليها بهذا المرسوم بقانون."

ومن خلال نص الفقرة الأولى من هذه المادة يتضح أن المشرع الإماراتي منح النائب العام سلطة وضع المتهم تحت المراقبة الإلكترونية أو حرمانه من استخدام شبكة الإنترنت في حال ارتكابه

[29]دولة الإمارات العربية المتحدة - مرسوم بقانون اتحادي - رقم ٣٤ لسنة ٢٠٢١ الصادر بتاريخ ٢٠٢١-٠٩-٢٠ نشر بتاريخ ٢٠٢١-٠٩-٢٦ يعمل به إعتبارا من ٢٠٢٢-٠١-٠٢ بشأن مكافحة الشائعات والجرائم الإلكترونية. الجريدة الرسمية ٧١٢ ملحق - السنة الواحد والخمسون

لأية جريمة من جرائم أمن الدولة المعلوماتي، كما أنه منح النائب العام إضافة إلى سلطة التحقيق في جرائم أمن الدولة المعلوماتي سلطة إخضاع المتهم في برامج التأهيل وفق ما يراه مناسباً.

ومن خلال نص الفقرة الثانية من هذه المادة أنه في حال بين التحقيق مع المتهم أنه مدان في إحدى جرائم أمن الدولة المعلوماتي أن يامر النائب العام بحجب المواقع الإلكترونية التي ارتكبي بها جريمة المساس بأمن الدولة المعلوماتي،"

نتيجة للانتشار المطرد في الجرائم الإلكترونية بشكل عام وجرائم أمن الدولة المعلوماتي على وجه الخصوص نتيجة الميزات التي تقدمها شبكة الإنترنت والتطبيقات المعلوماتية الحديثة، قرر وزير العدل في دولة الإمارات العربية المتحدة إنشاء نيابة عامة اتحادية متخصصة في مجال جرائم أمن الدولة المعلوماتي التي يجرمها مرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ بشأن الشائعات والجرائم الإلكترونية، حيث صدر قرار وزير العدل رقم (١٣٤) لسنة ٢٠٢٢ على انه:" ينشأ بمكتب النائب العام نيابة متخصصة تسمى "النيابة الاتحادية لمكافحة الشائعات والجرائم الإلكترونية". وهذه النيابة الاتحادية متخصصة في مجال الجرائم الإلكترونية الماسة بأمن الدولة، حيث تشكلت من (رئيس النيابة) وعدد من أعضاء النيابة العامة وعدد من الخبراء من الفنيين والقانونين، ومن بينهم وكلاء نيابة ومعاونون في إمارات الدولة كافة تحت إشراف النائب العام، وتعمل هذه النيابة على البحث والتحري عن الجرائم الإلكترونية الماسة بأمن الدولة المعلوماتي، وذلك لتخطي العوائق التي تواجه عمليات التفتيش الإلكتروني، وضبط المعطيات التي تحتويها الأنظمة الإلكترونية.

وبعد صدور مرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ تم تحويل كافة ملفات التحقيق في جرائم أمن الدولة المعلوماتي إلى هذه النيابة العامة، حيث أصبحت هذه النيابة تتمتع بشرعية إجرائية فيما يتعلق بتفتيش النظم الإلكترونية وعمليات الضبط والحجز والتحقيق في الجرائم الماسة بأمن الدولة المعلوماتي، كما أصبحت تتمتع بشرعية تجريمية، حيث أصبحت تتمتع بإعطاء التكييف المناسب للجريمة الإلكترونية الماسة بأمن الدولة المعلوماتي.

المبحث الثالث

تحديات التحقيق في جرائم أمن الدولة المعلوماتي

نتناول في هذا المبحث تحديات التحقيق في جرائم أمن الدولة المعلوماتي من خلال ثلاثة مطالب على النحو التالي:

- المطلب الأول: طبيعة مرتكبي جرائم أمن الدولة المعلوماتي
- المطلب الثاني: طبيعة الوسائل المستخدمة في ارتكاب جرائم أمن الدولة المعلوماتي
- المطلب الثالث: التحديات المرتبطة بالدليل الخاص بالجريمة

المطلب الأول

طبيعة مرتكبي جرائم أمن الدولة المعلوماتي

المجرم السيبراني أو مرتكب الجرائم السيبرانية هو شخص يختلف كثيراً عن المجرم التقليدي الذي تناولته نظريات علم الإجرام بالتحليل والتعريف والتصنيف.

مرتكب الجريمة السيبرانية شخص يتميز بالذكاء والإلمام بعلوم ومعارف التقنيات العالية للمعلومات والاتصالات، قد يكون المجرم هنا مهنياً أو خبيراً أو موظفاً كبيراً في المؤسسة أو الموقع الذي يرتكب فيه جريمته السيبرانية،وقد يكون باحثاً أو هاوياً يختبر قدراته وبرامجه الخاصة لاختراق المواقع أو اكتشاف الأسرار الخاصة بالغير المخزنة في قواعد البيانات.

فمرتكب الجرائم السيبرانية ليس مجرماً بالميلاد أو مجرماً بالصدفة أو شخصاً دفعته الظروف الاجتماعية والاقتصادية كما تقول نظريات علم الاجرام.[30]

فمرتكب الجريمة السيبرانية - في الغالب - من الطبقة الاجتماعية الوسطى، نال قدراً من التعليم والتأهيل واكتسب مهارات معلوماتية يعيش في وضع اجتماعي يسمح له بالتعامل مع أجهزة الحاسب الآلي وبرامجه، فهو رغم سلوكياته السلبية يُعد ثروة قومية ينبغي حسن استغلاله. ومن هنا يكون من الضروري التعامل معه

[30] جميل زكريا، الأمن والانترنت، ورقة عمل مقدمة بندوة الأمن والإنترنت، أكاديمية الشركة (مركز بحوث الشرطة)، القاهرة، ٢٠٠٣/٦/١٥.

كمجرم متميز. فالتحقيق معه ليس بالسهل لذكائه ولغته التي قد لا يفهمها المحقق العادي، سواءً أكان شرطياً أو وكيلاً للنيابة أو قاضياً. كما أن العقوبات التقليدية كالحبس والسجن والغرامة وغيرها من السياسات العقابية السائدة لا تصلح لردعه أو إصلاحه والاستفادة من طاقاته الكامنة[31]

هناك أمور تعيق سلطات التحقيق في جرائم أمن الدولة المعلوماتي، أثناء ممارستها لإجراءات التحقيق في هذا النوع من الجرائم،وتتمثل هذه الأمور بما يأتي[32]:

١) اختفاء آثار الجريمة الواقعة على أمن الدولة المعلوماتي وغياب الدليل المرئي الممكن بالقراءة فهمه، إذ إن مرتكبي هذا النوع من الجرائم نادراً ما يتركون آثاراً مادية ملموسة يمكن أن تشكل طرف خيط يقود إليهم بفضل مهاراتهم في استخدام هذه التقنيات وبرامجها.
٢) صعوبة الوصول إلى الدليل الإلكتروني في جرائم أمن الدولة المعلوماتي لكون مرتكب جريمة أمن الدولة المعلوماتي يحيط الأدلة بوسائل الحماية الفنية كاستخدام كلمات السر حول مواقعهم تمنع الوصول إليها أو تشفيرها لإعاقة المحاولات الرامية إلى الوصول إليها والإطلاع على محتواها أو استنساخها.
٣) سهولة محو الدليل في جرائم أمن الدولة المعلوماتي أو تدميره في زمن قصير، فالجاني يُمكنه محو الأدلة التي تكون قائمة ضده أو تدميرها في زمن قصير جداً، بحيث يصعب على الجهات التحقيقية كشف الجريمة إذا علمت بها.
٤) الضخامة البالغة لحجم المعلومات والبيانات المتعين فحصها في جرائم امن الدولة المعلوماتي وامكانية خروجها عن نطاق اقليم الدولة[33].
٥) لا يستخدم مرتكبي جرائم امن الدولة المعلوماتي في دخولهم شبكة الانترنت أجهزتهم الخاصة في أغلب الأحيان، وإنما يلجأون إلى مقاهي الانترنت المنتشرة حالياً في معظم المدن والأحياء التي لا تتقيد بأي ضوابط أو أنظمة أمنية يُمكن من خلالها التعرف على مستخدمي أجهزة الحاسب الآلي المتعاقبين في حالة اكتشاف أفعال غير مشروعة مصدرها هذه الأجهزة.

---

[31]د. ضاحي خلفان تميم: الإنترنت رؤية امنية، بحوث ودراسات شرطية، مركز البحوث والدراسات، القيادة العامة لشرطة دبي، العدد (٥٧)، سبتمبر ١٩٩٦، ص ٢.

[32]د. حسني الجندي: التشريعات الجنائية الخاصة في دولة الإمارات العربية المتحدة، الكتاب الثالث، بدون دار نشر، ط١، ٢٠٠٩م، ٢٢٩.

[33] خالد عياد الحلبي: جرائم الإنترنت، دار النهضة العربية، القاهرة، ٢٠١٨، ص٢٢٣.

٦) أغلب البيانات والمعلومات التي يتم تداولها عبر الحاسب الآلي وشبكة الانترنت في جرائم امن الدولة المعلوماتي هي عبارة عن رموز مخزنة على وسائط ممغنطة لا يُمكن الوصول إليها إلا بواسطة الحاسب الآلي ومن قبل أشخاص قادرين على التعامل مع هذه الأجهزة ونظمها[34].

فهناك صعوبة في ملاحقة مرتكب هذه الجرائم، ولو تم التوصل إليه فمن السهل اتلاف الأدلة من قبل الجناة، كما أن هذه الجرائم لا تحدها حدود فهي جرائم عابرة للحدود مما يثير تحديات ومعوقات في حفل الاختصاص القضائي والقانون الواجب التطبيق ومتطلبات التحقيق والملاحقة والضبط والتفتيش.

كما أن الدافع لارتكاب جرائم الإنترنت يختلف عن دافع الجرائم التقليدية، فالبعض يرتكب الجريمة الإلكترونية لولعه في الحصول على المعلومات الجديدة مثل القراصنة، أو للاستيلاء على المعلومات الموجودة على جهاز الكمبيوتر أو حذفها أو تدميرها أو إلغائها نهائياً، وقد يكون الدافع الرغبة في قهر النظام الإلكتروني بغرض تحقيق شهرة وإثبات التفوق العلمي لديه وهي تكون بين الشباب، وقد تكون لاستهداف بعض الأشخاص والجهات.[35]

المطلب الثاني

طبيعة الوسائل المستخدمة في ارتكاب جرائم أمن الدولة المعلوماتي

لقد صاحب التطور الذي شهده العالم في الفترة الأخيرة من القرن الماضي وحتى يومنا هذا في شتى المجالات تطوراً فيما يتعلق بوسائل التقنيات الحديثة تمثلت بظهور الشبكة الدولية للمعلومات (الإنترنت) كإحدى صور التقنيات الحديثة واهمها، بكافة وسائل استخدامها وكافة النتائج الإيجابية والسلبية الناشئة عن استخدامها[36].

---

[34] راشد بشير ابراهيم: الجرائم الإلكترونية، دار وائل، عمان، ٢٠١٩، ص٩٠.

[35]دكتور خالد سامي السيد : الأمن القومي الإلكتروني وجرائم المعلومات– دار النهضة العربية – القاهرة – مصر – الطبعة الأولى – ٢٠٢١ – ص٧٤

[36] د. محمد عبيد الكعبي: الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت، دار النهضة العربية، القاهرة، ٢٠٠٥م، ص ٩.

فأصبحت وسائل التقنيات الحديثة من أكثر الوسائل استخداماً في ارتكاب الجرائم بكافة أنواعها، وفي مقدمتها الجرائم الماسة بأمن الدولة من جهة الخارج. وأصبحت وسائل التقنيات الحديثة بمتناول أيدي الجميع، فهي لا تتقيد بالحدود المكانية للدول أو الحدود الزمانية أيضاً، وهذه الميزة جعلت وسائل التقنيات الحديثة الأكثر استخداماً في المساس بأمن الدولة من جهة الخارج.

حيث يقوم الجناة بارتكاب الجريمة باستخدام وسائل التقنيات الحديثة، وخاصة تلك التقنيات التي توفر ميزة الاتصال وكذلك شبكات التواصل الاجتماعي والتقنيات الحديثة التي يمكن التحكيم بها عن بعد والتي توفر إمكانية نقل الصور والخرائط والاحداثيات والمواقع الهامة في الدولة.

وقد تنوعت التقنيات الحديثة التي تستخدم كوسيلة لارتكاب الجرائم الماسة بأمن الدولة من جهة الخارج[37] فظهرت على سبيل المثال الأقمار الصناعية التي يتم فيها التحكم عن بعد وتستخدم لتصوير المواقع الحساسة في الدولة وظهرت أيضا التقنيات الحديثة الخاصة بالاستشعار عن بعد والتي تحتوي خاصية تحديد المواقع باستخدام التقنيات الحديثة، بالإضافة الى ظهور طيارات بدون طيار الحديثة والتي تستخدم لأغراض التجسس والتصوير كم ظهرت وسائل الاعلام الحديثة التي تعمل على شبكة الانترنت كإحدى الوسائل التي تستخدم في الجرائم الماسة بأمن الدولة من جهة الخارج.

وللتعرف على أهم التقنيات الحديثة التي تستخدم في ارتكاب الجرائم الواقعة على أمن الدولة[1] فكان من المستجدات في عالم التطور والثورة المعلوماتية الحديثة دخول الحاسبات الآلية (أنظمة الكمبيوتر) وشبكات الإنترنت عالم الجريمة، تماماً كما هو الشأن في الجرائم المنظمة وفي مقدمتها جرائم امن الدولة المعلوماتي ، فهي في الحقيقة ليست مجرد جرائم تقليدية بطبيعتها في ثوب جديد أو بوسيلة معينة[48]، وهذا التعبير وإن صح فإنه قد ينطبق على الجرائم الإلكترونية والتي يكون فيها الحاسب الآلي أو شبكات الاتصال مجرد وسيلة لارتكاب السلوك الإجرامي في هذا المجال كاتصال أفراد العصابات الخطيرة المنظمة لبعضهم البعض لتبادل وتدبير جرائمهم المختلفة في أماكن متفرقة داخل البلاد أو على الصعيد الدولي، مثل قضايا الإرهاب على اختلاف توجهاتها،

(37)

[1] حسن البلوشي: جرائم أمن الدولة الخارجي باستخدام التقنيات الحديثة، رسالة ماجستير، أكاديمية شرطة دبي، دبي، ٢٠١٧، ص ٧٩

(48)

والاتجـار وتهريـب المخـدرات والمـواد الضـارة والمشـعة، والاتجـار فـي الرقيـق والأعضـاء البشـرية، وشـبكات الـدعارة والبغـاء، والسـرقات الكبـرى للبنـوك والمؤسسـات الماليـة والاقتصـادية، والاتجـار فـي الأسـلحة والـذخائر بطـرق غيـر مشـروعة، كـل ذلـك بـدء فـي مطلـع السـتينيات والسـبعينيات مـن القـرن السـابق (العشـرين)، ويمكـن القـول بحـق هنـا - أن هـذا النـوع مـن الجـرائم لـه نمـط جديـد فـي محتـواه الإجرامـي وحجمـه وخطورتـه ووسـائله غيـر التقليديـة، ومشـاكله المعقـدة، فلـه سـمات وطبيعـة خاصـة وأيضاً في سمات وطبائع مرتكبيها[39].

وهنـاك بعـض التحـديات التـي تواجـه جهـات التحقيـق فـي جـرائم امـن الدولـة المعلومـاتي، ولا سـيما أن مرتكبـي الجـرائم يسـتخدمون أنظمـة معلوماتيـة متطـورة يصـعب فـي بعـض الأحيـان التعامـل معهـا مـن قبـل جهـة التحقيـق، وعليـه نبـين فـي هـذا المطلـب التحـديات المتعلقـة بوسـائل ارتكـاب هـذه الجـرائم علـى النحو الآتي:

أولاً: نوعية الوسائل المستخدمة في ارتكاب الجريمة

فيمـا يتعلـق بجـرائم أمـن الدولـة المعلومـاتي ، فالأصـل فيهـا، أن كـل جريمـة منهـا تـتم باسـتخدام أو عبـر الوسـائل الإلكترونيـة الحديثـة، وهـي جريمـة إلكترونيـة معلوماتيـة تمـس أمـن الدولـة، لكـن العكـس غيـر صـحيح [40] وإن التقـدم السـريع والتطـورات المتلاحقـة فـي مجـال تكنولوجيـا المعلومـات والاتصـالات، ومـا يواكبـه مـن مسـتجدات وتطـورات مماثلـة علـى صـعيد الجـرائم الدوليـة عمومـاً، وجـرائم أمـن الدولـة المعلومـاتي خصوصـاً مـن حيـث أسـاليب ارتكابهـا ووسـائلها وأنواعهـا وآثارهـا بصـفة خاصـة، باتـت تفـرض علـى المشـرع الـوطني، بـين الحـين والآخـر، مواكبـة ذلـك باسـتحداث نصـوص جديـدة أو تعـديل نصوص حالية لضمان كفاءة وفعالية هذه النصوص في مكافحة الجرائم محل الاهتمام.

---

[39] بـين جيـتس: "المعلوماتيـة بعـد الإنترنـت طريـق المسـتقبل" - ترجمـة أ. عبـد السـلام رضـوان، إصـدار المجلـس الوطني للثقافة والفنون والأدب، الكويت، سلسلة عالم المعرفة - العدد٢٣١، ص٧.

[40] راجـع فـي شـأن العلاقـة بـين الجـرائم السـيبرانية/ الإلكترونيـة والإرهـاب السـيبراني، علـى سـبيل المثـال: دراسـة شـاملة عـن الجريمـة السـيبرانية، فيينـا: مكتـب الأمـم المتحـدة المعنـي بالمخـدرات والجريمـة، فبرايـر ٢٠١٣م، ص١٣، متاح على الرابط:

https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Study_Arabic.pdf .

ممـا أسـفر عـن اعتمـاد المشـرع الـوطني، لـبعض التعـديلات المتلاحقـة أو اسـتحداث نصـوص جديـدة لتجـريم أفعـال معينـة تمـس بعـض جوانـب ظـاهرة المسـاس بـأمن الدولـة المعلومـاتي فـي السـنوات العشرين الأخيرة[41].

وتجـدر الإشـارة إلـى أن المعلومـات الإلكترونيـة تشـمل كـل مـا يمكـن تخزينـه ومعالجتـه وتوليـده، ونقلـه بوسـائل تقنيـة المعلومـات، وبوجـه خـاص الكتابـة والصـور، والصـوت والأرقـام والحـروف والرمـوز والإشـارات وغيرهـا أمـا البرنـامج المعلومـاتي الإلكترونـي فهـو مجموعـة مـن البيانـات والتعليمـات والأوامـر القابلـة للتنفيـذ بوسـائل تقنيـة المعلومـات وممتـدة لإنجـاز مهمـة مـا. ونظـام المعلومـات الإلكترونـي عبـارة عـن مجموعـة بـرامج وأدوات محـددة لمعالجـة وإدارة البيانـات أو المعلومـات أو الوسائل الإلكترونية أو غير ذلك[42].

ثانياً: وسائل ارتكاب جرائم امن الدولة المعلوماتي تختلف من جريمة لأخرى.

أفـرزت الثـورة المعلوماتيـة الحديثـة نوعـاً جديـداً مـن الجـرائم الماسـة بـأمن الدولـة المعلومـاتي، وهـو مـا يسـمى بـالجرائم الرقميـة أو الجـرائم المعلوماتيـة الماسـة بـامن الدولـة المعلومـاتي والتـي تمثـل أنماطـاً متعـددة مـن السـلوك الإجرامـي تـتم مـن خـلال الأجهـزة الحاسـوبية والشـبكة المعلوماتيـة، وحيـث إن الجريمـة الرقميـة الماسـة بـأمن الدولـة ترتكـب فـي عـالم افتراضـي فقـد أُثيـر التسـاؤل حـول مـدى تطـور إجـراءات التحقيـق الجنـائي حتـى يمكـن التعامـل مـع هـذا النـوع الجديـد مـن الإجـرام حيـث إنهـا تخضـع بالضـرورة لإجـراءات تختلـف عـن القواعـد الإجرائيـة التقليديـة لاسـتخلاص الـدليل الجنـائي، ولـذلك بـدت أهميـة موضـوع التحقيـق الجنـائي الرقمـي القـائم علـى التحليـل الجنـائي الرقمـي باسـتخدام التقنيـات التكنولوجيـة الحديثـة، للحصـول علـى مـا يسـمى بالـدليل الرقمـي فـي جـرائم امـن الدولـة المعلومـاتي وتحقيقه بالطرق المثبتة علمياً والتي تؤكد على ضرورة مشروعيته**(43)**

---

[41]دكتـورة هالـة أحمـد الرشـيدي : الإرهـاب السـيبراني ـــ دار النهضـة العربيـة – القـاهرة – مصـر – الطبعـة الأولـى – ٢٠٢١م – ص٩٣

[42] المـادة مـن القـانون الاتحـادي رقـم (٢) لسـنة ٢٠٠٦م فـي شـأن مكافحـة جـرائم تقنيـة المعلومـات لدولـة الإمـارات العربية المتحدة.

[43]حنـان محمـد الحسـيني، وسـحر علـي عبداللـه الهبـدان. "التحقيـق الجنـائي الرقمـي". مجلـة جامعـة الملـك سـعود - الحقـوق والعلـوم السياسـية مـج ٣٣، ع٢، (٢٠٢١): ص١٢٩ الـدكتور راشـد محمـد المـري : الجـرائم الإلكترونيـة فـي ظـل الفكـر الجنـائي المعاصـر– دار النهضـة العربيـة للنشـر والتوزيـع – القـاهرة – مصـر – الطبعـة الأولـى – ٢٠١٨م – ص٧٥

ثالثاً: وسائل ارتكاب جرائم أمن الدولة المعلوماتي تنعكس على الأدلة

تبدأ المشكلات الإجرائية في مجال جرائم أمن الدولة المعلوماتي بتعلقها في كثير من الأحيان ببيانات معالجة إلكترونياً وكيانات منطقية غير مادية، وبالتالي يصعب من ناحية كشف هذه الجرائم، ويستحيل من ناحية أخرى في بعض الأحيان جمع الأدلة بشأنها، وما يزيد من صعوبة الإجراءات في هذا المجال سرعة ودقة تنفيذ الجرائم الإلكترونية وإمكانية محو آثارها، وإخفاء الأدلة المتحصلة عنها عقب التنفيذ مباشرة[44].

ويواجه التفتيش وجمع الأدلة صعوبات كثيرة في هذا المجال، لأنهما قد يتعلقان ببيانات مخزنة في أنظمة أو شبكات إلكترونية موجودة بالخارج، ويثير مسألة الدخول إليها ومحاولة جمعها إلى الدولة التي يجري فيها التحقيق، مشكلات تتعلق بسيادة الدولة أو الدول الأخرى التي توجد لديها هذه البيانات، وفي هذه الحالة يحتاج الأمر إلى تعاون دولي في مجالات البحث والتفتيش والتحقيق وجمع الأدلة وتسليم المجرمين، بل وتنفيذ الأحكام الأجنبية الصادرة في هذا المجال[45].

المطلب الثالث

التحديات المرتبطة بالدليل الخاص بالجريمة

هناك بعض التحديات التي تواجه جهة التحقيق في جرائم أمن الدولة المعلوماتي، من حيث الأدلة الخاصة بالجريمة، ونبين في هذا المطلب تلك التحديات على النحو التالي:

أولاً: صعوبة تحديد الأدلة في جرائم أمن الدولة المعلوماتي.

جرائم امن الدولة المعلوماتي من طائفة الجرائم الإلكترونية الماسة بأمن الدولة التي نص عليها المشرع الإماراتي في مرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ بشان مكافحة الشائعات والجرائم الإلكترونية، حيث تتصف الجريمة الإلكترونية الماسة بأمن الدولة المعلوماتي بأنها صعبة الإثبات ولكن ليست مستحيلة الإثبات وأساس ذلك أن الجاني في كثير من الأحيان مجهول، خاصة في تلك النوعية من الجرائم التي تتعلق بوسائل الاتصال وليس بالحاسب الآلي بصورة

---

[44] أحمد حسام طه تمام، المرجع السابق، ص١٨. دكتور خالد سامي السيد : الأمن القومي الإلكتروني وجرائم المعلومات– دار النهضة العربية – القاهرة – مصر – الطبعة الأولى – ٢٠٢١ – ص ٥٦

[45] . www.arablawinfo.com/Researches_AR/126.doc

مجردة من اتصاله بتلك الشبكات، إذ أن الجاني يستخدم وسائل فنية وتقنية في كثير من الأحيان كما أن الفعل المكون للركن المادي للجريمة والذي يمثل السلوك الإجرامي لا يستغرق وقتاً طويلاً بل في مجرد ثوان (Cyber Crime) ويتم في الخفاء[46] ومؤدى ذلك أن الجرائم المعلوماتية الماسة بامن الدولة المعلوماتي في أكثر صورها خفية[47].

وهناك صعوبات أخرى أيضاً تكمن في صعوبة الاحتفاظ الفني بدليل الجريمة المعلوماتية؛ إذ يستطيع المجرم المعلوماتي في أقل من ثانية أن يمحو أو يحرف أو يغير البيانات والمعلومات الموجودة في الكمبيوتر، لذا فإن للمصادفة وسوء الحظ دوراً في اكتشافها يفوق دور أساليب التدقيق والرقابة ومعظم مرتكبي الجريمة المعلوماتية الذين تم ضبطهم وفقاً لما لاحظه أحد الخبراء في الجريمة المعلوماتية إما أنهم تصرفوا بغباء أو لم يستخدموا الأنظمة المعلوماتية بمهارة[48].

فالجريمة الإلكترونية تتم في بيئة غير تقليدية حيث تقع خارج إطار الواقع المادي الملموس لتقوم أركانها في بيئة الحاسوب والإنترنت مما يجعل الأمور تزداد تعقيداً لدى سلطات الأمن وأجهزة التحقيق والملاحقة. ففي هذه البيئة تكون البيانات والمعلومات عبارة عن نبضات إلكترونية غير مرئية تنساب عبر النظام المعلوماتي ما يجعل طمس الدليل كلياً من قبل الفاعل سهلاً[49].

ويوجد صعوبة في إثبات الجريمة الإلكترونية تمكن في الجناة مرتكبي تلك الجرائم الذين يتسمون بالذكاء والدهاء والخبرة التقنية أثناء ارتكابها، إضافة إلى عدم ملائمة الأدلة والتقنية في القانون الجنائي[50]

فصعوبة إثبات هذه الجريمة يرجع إلى عدة أسباب من بينها وسيلة تنفيذها والتي تتسم في أغلب الحالات بالطابع التقني الذي يضفي عليها الكثير من التعقيد. بالإضافة إلى الإحجام عن الإبلاغ

---

(46) الدكتور عماد مجدي عبد الملك: جرائم الكمبيوتر والانترنت، دار المطبوعات الجامعية، ٢٠١١م، ص٤٣.

(47)محمد علي سويلم : مكافحة الجرائم الإلكترونية ـــ دار المطبوعات الجامعية – القاهرة – مصر – الطبعة الأولى – ٢٠١٩م – ص١٧ إلى٣٩ – ص٩٠ إلى١٢١ – ص٣١

(48) الدكتور محمد عبد الله أبو بكر: جرائم الكمبيوتر والإنترنت، منشأة المعارف، ٢٠٠٦م، ص٩٥.

(49) الدكتور خالد ممدوح إبراهيم: الجرائم المعلوماتية، دار الفكر الجامعي، ٢٠٠٩م، ص٤٣.

(50) الدكتور محمد عبد الله أبو بكر سلامة: المرجع السابق، ص٩٩.

عنهـا فـي حالـة اكتشـافها لخشـية المجنـي عليـه مـن فقـد ثقـة عملائهـا، فضـلاً عـن إمكانيـة تـدمير المعلومات التي يمكن أن تستخدم كدليل في الإثبات في مدة قد تقل عن الثانية الواحدة[51].

ثانياً: صعوبة تعقب الأدلة في جرائم أمن الدولة المعلوماتي

جـرائم امـن الدولـة التـي ترتكـب عبـر الوسـائل التقنيـة الحديثـة تمتـاز بالتباعـد الجغرافـي [52]، يسـتخدم الجـاني فيهـا وسـائل فنيـة تقنيـة معقـدة فـي كثيـر مـن الأحيـان، كمـا يتمثـل السـلوك المجـرم المكـون للـركن المـادي فيهـا مـن عمـل سـريع، قـد لا يسـتغرق أكثـر مـن بضـع ثـوان، بالإضـافة إلـى سـهولة محـو الـدليل، والتلاعـب فيـه أمـام هـذا كلـه يبـرز صـعوبة الإثبـات فـي جـرائم التقنيـة، خصوصـاً مـع الافتقـار إلـى الدليل المادي التقليدي (دم، شعر، بصمة ...)[53].

تتميـز جـرائم أمـن الدولـة المعلومـاتي عـن الجـرائم التقليديـة بأنهـا صـعبة الإثبـات، حيـث أنهـا جريمـة لا تتـرك فـي الغالـب أثـراً ماديـاً ظـاهراً يمكـن ضـبطه، وسـهولة محـو الـدليل أو تـدميره فـي زمـن قصـير، يضاف إلى ذلك نقص خبرة الشرطة والنظام العدلي، وعدم كفاية القوانين القائمة[1].

وتجـدر الإشـارة علـى أن محـور الجريمـة هـي جريمـة المسـاس بـأمن الدولـة المعلومـاتي مـن خـلال إنشـاء مواقـع إلكترونيـة أو تطبيقـات لتلـك الغايـة، حيـث ترتكـب تلـك الجريمـة فـي بيئـة رقميـة، ولـذلك فـإن الجـاني بحاجـة إلـى اسـتخدام الحاسـوب، أو وسـيلة تكنولوجيـا معلومـات ليصـل إلـى مسـرح الجريمـة، كمـا تمـول الإرهـاب بطريقـة إلكترونيـة لا يحتـاج إلـى اللجـوء إلـى العنـف، وأمـا يتعلـق بالإثبـات فيكـاد أن يكـون الـدليل الرقمـي هـو الـدليل الوحيـد فـي هـذا النـوع مـن الجـرائم، وهـذا الـدليل يكـون عرضـة للتخريـب بسـهولة، مـع العلـم أن بعـض مرتكبـي جريمـة تمويـل الإرهـاب بطـرق إلكترونية قد يكونون أشخاصاً محترفين في مجال تكنولوجيا المعلومات[54].

---

[51] الدكتور هشام محمد فريد رستم: المرجع السابق، ص٥٥.

[52] هشام فريد رستم قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الكاتبة، ١٩٩٥م، ص٤١

[53] القاضـي الـدكتور أسـامة أحمـد المناع*سـة والقاضـي جـلال محمـد الزعبـي : جـرائم تقنيـة نظـم المعلومـات الإلكترونية ـــ دار الثقافة للنشر والتوزيع – عمان - الأردن – الطبعة الرابعة – ٢٠٢٢م – ص٣٨

[1]دكتـور خالـد حسـن أحمـد لطفـي : جـرائم الإنترنـت ـــ دار الفكـر الجـامعي – الإسـكندرية – مصـر – الطبعـة الأولـى – ٢٠١٨م – ص ٢٤

[54] عبـد اللـه بـن عبـد العزيـز العجـلان: الرهـاب الإلكترونـي فـي عصـر المعلومـات، بحـث متقـدم إلـى المـؤتمر الـدولي الأولحـول "حمايـة أمـن المعلومـات والخصوصـية فـي قـانون الإنترنـت"، والمنعقـد بالقـاهرة فـي المـدة مـن ٢-٤ يونيـو ٢٠٠٨م.

وقد سعت العديد من الدول إلى اتخاذ التدابير لمواجهة تمويل الإرهاب من خلال الشبكة الإلكترونية ، إلا أن هذه الجهود لا تزال بحاجة إلى المزيد من هذه الجهود المبذولة لمواجهة هذا الجريمة[55].

ثالثاً: التحديات التي تواجه الخبير في الحصول على الدليل في جرائم أمن الدولة المعلوماتي.

تلعب الخبرة في المجال الجنائي دوراً كبيراً في إظهار الحقيقة، ولا غنى عنها في كافة مراحل الدعوى الجزائية بل وقبل أن ترفع الدعوى الجزائية في مرحلة الاستدلال والتحري التي هي مجالنا في هذا الصدد، ويعتبر نص المادة ٤١ من قانون الإجراءات الجزائية الإتحادى الإماراتى السند القانوني لا ستعانة مأموري الضبط القضائي بالخبراء أثناء مرحلة الاستدلال والتحري فقد جاء فيها أنه : (... ولهم أن يستعينوا بالأطباء وغيرهم من أهل الخبرة ولا يجوز لهم تحليف الشهود أو الخبراء اليمين إلا إذا خيف ألا يستطاع فيما بعد سماع الشهادة)

. فقد تعرض مسألة أثناء قيام مأمور الضبط القضائي بإجراءات الاستدلال والتحري تحتاج إلى معرفة فنية أو علمية خاصة، وهنا يكون لمأمور الضبط القضائي أن يستعين بمن تتوافر لديه الخبرة المطلوبة، فقد أجازت المادة ٤١ لمأموري الضبط الاستعانة بالأطباء على وجه الخصوص في المسائل التي تحتاج إلى خبرة طبية كجرائم القتل والإيذاء والاعتداءات الجنسية وجرائم الإجهاض التي تستلزم الاستعانة فيها بالأطباء الشرعيين، وجاء في حكم لمحكمة تمييز دبي: (أن المادة ٤٠ من قانون الإجراءات الجزائية تجيز لمأموري الضبط القضائي أثناء جمع الأدلة أن يستعينوا بالأطباء وغيرهم من أهل الخبرة، ومن ثم فإن استعانة مأموري الضبط بقسم الطب الشرعي خشية ضياع أدلة الدعوى وتقديم الطبيب الشرعي تقريره وفق ما كلف به ليس فيه أية مخالفة للقانون)[56]

ويجوز الاستعانة بغيرهم من الخبراء في المجالات كافة، كالاستعانة بخبراء الأسلحة والمتفجرات وخبراء لتحديد سبب الحريق، وخبراء رفع البصمات وغيرهم من الخبراء، وبما أن هذه الخبرة

---

[55] أيسر محمد الجرائم عطية: المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، المتلقي العامي، ورقة علمية بعنوان: دور الآليات الحديثة للحد من الجرائم المستحدثة، الإرهاب الإلكتروني وطرق مواجهته، كلية العلوم الاستراتيجية، الأردن، ص١٠. الدكتور عبد الله ذيب محمود والدكتور أسامة إسماعيل دراج : الوجيز في الجرائم الإلكترونية ـــ دار الثقافة للنشر والتوزيع – عمان – الأردن - الطبعة الأولى – ٢٠٢٢م – ص٤٣

[56] محكمة التمييز - الأحكام الجزائية – الطعن رقم ٢١٧ – لسنة ٢٠٠٣ قضائية – تاريخ الجلسة ٢٠٠٣-١٠-١٨ – مكتب فني ١٤ – رقم الجزء ١ – رقم الصفحة ٢٤٩

من الإجراءات الاستدلالية يجب عدم مساسها بالحرية الشخصية للأفراد، ولا يجوز لمأمور الضبط القضائي تحليف الخبير اليمين القانونية إلا إذا خشي عدم إمكانية سماع شهادته حول ما جاء في تقرير الخبرة في المراحل التالية وهي حالة تكاد تكون نادرة الحدوث في حالة الخبرة بخلاف الشهادة، فالخبير الذي يخشى عدم إمكانية سماع شهادته يمكن الاستعانة بغيره من الخبراء بينما لا يجوز ذلك بالنسبة للشاهد ؛ لأن الشهادة تقوم على الاعتبار الشخصي بخلاف الخبرة التي تقوم على الاعتبار الفني والعلمي.[57]

ويلتزم الخبير في هذه الحالة أن يكون ملما بمكونات الحاسوب المادية، والشبكات الإلكترونية، والأنظمة الحاسوبية، ووسائل التكنولوجيا المختلفة، وكذلك إلمامه بكيفية الربط بين الدليل المادي والإلكتروني في الوقائع محل البحث وكذلك فهمه للبيئة التي يعمل فيها، وكذلك قدرته على أداء مهامه الموكلة، دون أن يترتب ضرراً على الدليل المراد الحصول عليه وبالتالي يجب على الخبير استخدام الأساليب المشروعة كافةً، لاكتشاف الدليل الذي يوصل للحقيقة وتمر أساليب الخبير الإلكتروني في تقصي الحقيقة بثلاث مراحل[58]:

المرحلة الأولى: تجميع المعلومات المخزنة لدى مقدم الخدمة من خلال تتبع أجهزة الحاسوب، أو الهواتف النقالة الحديثة التي دخل منها المجرم لتتبع آثاره.

المرحلة الثانية: مرحلة المراقبة، وتتم من خلال برامج خاصة يمكن بواسطتها حصر بيانات الدخول والخروج من المواقع الإلكترونية التي لها علاقة بالجريمة المرتكبة.

وتتم بفحص معلومات النظام المادية والمعنوية كافة، لاستخراج الأدلة وتقديمها لجهات التحقيق، ومعرفة مدى وقوع الجريمة باستخدام النظام محل الضبط من عدمه.

ويواجه الخبير الجنائي صعوبات متعددة عند قيامه بمهامه المتمثلة بجمع الأدلة الإلكترونية في جرائم امن الدولة المعلوماتي[59] منها:

---

[57] إيهاب عبد المطلب: جرائم الإرهاب داخلياً وخارجياً في ضوء القضاء والفقه، المركز القومي للإصدارات القانونية، القاهرة، ط١،٢٠٠٩م، ص ٢٧.

[58] نداء المصري: خصوصية الإثبات في الجرائم المعلوماتية، رسالة ماجستير، جامعة النجاح الوطنية، نابلس، ٢٠٠٧م، ص٦٠.

[59] عبد الفتاح حجازي: القانون الجنائي والتزوير في جرائم الحاسوب والانترنت، دار الكتب القانونية، مصر، ٢٠٠٥م، ص٢٤.

١- فقد جزء كبير من المعلومات عند إغلاق الجهاز، أو قطع التيار الكهربائي عنه، فقد يؤدي هذا الإجراء لمحو العديد من المعلومات عن ذاكرة الجهاز، أو تحريف بيانات مهمة؛ نتيجة حدوث ضرر في الجهاز، ومنع التحميل، وبالتالي فقدان أدلة مهمة.

٢- قيام الجاني بتهيئة الجهاز للتدمير بمجرد تشغيله.

٣- طبيعة مسرح الجريمة، فالشبكات الإلكترونية منتشرة في أماكن متعددة وفي عدة دول، وبالتالي قد لا يتمكن الخبير من الحصول على الدليل نتيجة معيقات تشريعية وإجرائية، كما أن سرعة مرور البيانات عبر الشبكات وحجم البيانات الضخمة التي تمر عبر الشبكات قد يمكن المجرمين من تدمير الأدلة، مما ينعكس على عمل الخبير في الحصول عليها.

٤- إخفاء الهوية، حيث يتعمد المستخدم إخفاء هويته سواء القيام ببعض الإجراءات، أو استخدام بعض البرامج، مما يشكل عائقاً أمام الخبير وتتبعها أمراً بالغ الصعوبة أمام الخبير الفني.

٥- إخفاء المعلومات، فوجود بعض البرامج الخاصة بإخفاء المعلومات، يؤدي لخلق نظام ملفات آمن عبر استخدام الإنترنت، مما يجعل عملية استعادة الأدلة، وتتبعها أمراً بالغ الصعوبة أمام الخبير الفني.

ويرى جانب من الفقه أن الخبير في مجال الأدلة الإلكترونية، يجب أن يكون ملماً بالأمور الآتية[60]:

١- أنظمة الحواسيب والهواتف النقالة والشبكات الإلكترونية.

٢- طرق الحماية من الاختراق والأمن المعلوماتي.

٣- معرفة تقنية عالية ببرامج التتبع وكشف الهوية.

٤- القدرة على التعامل مع مسرح الجريمة الإلكترونية واستخلاص الأدلة التقنية منه.

٥- كيفية تفسير الملاحظات واستخلاص النتائج ذات الأهمية العلمية والقضائية.

---

[60] عبد الناصر محمد فرغلي، ومحمد عبيد المسماري: بحث بعنوان الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية مقدم للمؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، جامعة نايف للعلوم الأمنية، الرياض، في الفترة ما بين ٢-١٤٢٨/١١/٤، ص٣٣.

ففي بعض الجرائم السيبرانية تكون الأدلة مخزنة ومصنفة في ملفات واضحة أما في جرائم أخرى قد لا يكون المحقق محظوظا ليجد مثل هذه الأدلة بالكيفية التي يتمناها، لأن الجناة يقومون بمحو البيانات وإغلاق الملفات التي تحتوي على الأدلة التي يمكن أن تدينهم. وفي بعض الأحيان لا يتم تخزين البيانات الهامة على الديسك توب ولكن هنالك قدراً كبيراً من البيانات يتم تخزينها في مواقع أخرى مثل Swap page-Cache files أو الملفات المؤقتة.

في هذا الجزء نحاول بيان الكيفية التي تمكن المحقق من استرجاع مثل هذه البيانات التي تم محوها أو تلك التي تم تخزينها في حقول غير تقليدية وتعرف مثل هذه البيانات أحياناً بـ Electronic dumpster diving. فإن عدداً كبيراً من مستخدمي الحاسب الآلي ومرتكبي الجرائم السيبرانية، وحتى خبراء الحاسب الآلي يعتقدون أن محو الملفات وإلغاء محتويات سلة المهملات تعني نهاية تلك البيانات[61].

ولكن ذلك ليس صحيحاً. فإن محو الملفات لا يعني إزالة محتوياتها نهائياً من الحاسب الآلي، بل يعني مجرد سحب مؤشرات تلك الملفات أو جدول الملفات الرئيسي. والحقيقة أن البيانات مخزنة على القرص الصلب في شكل clusters وهي وحدات تتكون من مجموعة أرقام من البتس.

و توجد بيانات الملفات التي يتم محوها مبعثرة في القرص الصلب في عدة مواقع، ولا شك أن سحب المؤشر عنها يجعل من الصعب إعادة جمع بياناتها، ولكن ليس من المستحيل استرجاع كل ذلك إلى حالتها الطبيعية. هنالك برامج عديدة تساعد على استرجاع الملفات المفقودة، وفي كثير من الحالات تكون هنالك بيانات قيمة مخفية في الحاسب الآلي، كما أن هنالك العديد من المواقع التي يمكن إخفاء الملفات فيها. ورغم أنه من الصعب إيجاد مثل هذه البيانات، إلا أنها تكون مفيدة أحياناً، وتستحق أن يبذل الجهد في استرجاعها[62].

وفي نهاية الطلب يستنتج الباحث أن مسألة التحديات التي تواجه جهة التحقيق في جرائم امن الدولة المعلوماتي فيما يخص الأدلة في الجريمة يمكن التغلب عليها من خلال التدريب المستمر للنيابة العامة والفنيين الملحقين بها في التعامل مع هذا النوع من الجرائم، والاستفادة من خبرات الدول

---

[61]محمد سعيد العامري : الأمن السيبراني والتحقيقات الرقمية ـــ المطبعة المتحدة للطباعة والنشر – أبو ظبي – الإمارات العربية المتحدة – الطبعة الأولى – ٢٠٢١م – ص١٥٥

[62]محمد سعيد العامري : الأمن السيبراني والتحقيقات الرقمية ـــ المطبعة المتحدة للطباعة والنشر – أبو ظبي – الإمارات العربية المتحدة – الطبعة الأولى – ٢٠٢١م – ص١٥٥

المتقدمة في هذا المجال، وينوه الباحث إلى أن دولة الإمارات العربية المتحدة من الدول المتقدمة في هذا المجال.

في نهاية المبحث الثالث يرى الباحث أن التحديات التي تواجه جهات التحقيق في جرائم أمن الدولة المعلوماتي جميعها تقوم على ثلاث أفكار رئيسية ، **الفكرة الأولى** هي أن مرتكب جرائم أمن الدولة المعلوماتي من طائفة المجرمين من ذوي الخبرة والاختصاص في التقنيات المعلوماتية الحديثة وهنا نرى انه من الضروري أن يتم التحقيق وفق تقنيات حديثة تقوف تلك التي يستخدما مرتكب الجريمة وهو ما يعطي التحقيق في هذا النوع من الجرائم خصوصية خاصة بها.

الفكرة الثانية: إن الوسائل المستخدمة في ارتكاب جرائم امن الدولة المعلوماتية هي تقنيات حديثة ومتطورة مع الوقت حيث أصبح الذكاء الاصطناعي يستخدم بشكل كبير في ارتكاب هذه الجرائم، وعليه هناك ضرورة لان يتم مواكبة كافة البرامج والتطبيقات الذكية التي من المحتمل أن تعتبر وسيلة لارتكاب الجرائم الماسة بأمن الدولة المعلوماتي، الأمر الذي يعطي التحقيق في هذا النوع من الجرائم خصوصية تختلف عن التحقيق في الجرائم التقليدية.

الفكرة الثالثة: إن الأدلة على ارتكاب الجرائم الماسة بأمن الدولة المعلوماتي من الممكن طمسها او تدميرها او حتى حذفها، كما ان الجرائم الماسة بامن الدولة المعلوماتي ترتكب في بعض الأحيان من جهات خارج الدولة الأمر الذي يجعل جهات التحقيق غير قادرة على تعقب مرتكب الجريمة ويمكن التغلب على هذه العقبة من خلال التعاون الأمني والتعاون القضائي بين الدولة والدول الأخرى.

الخاتمة

تناول البحث خصوصية التحقيق في جرائم أمن الدولة من حيث تعريف التحقيق ، والجهة القائمة على التحقيق في هذا النوع من الجرائم، والتحديات التي تواجه جهات التحقيق في جرائم أمن الدولة المعلوماتي، وفي نهاية البحث توصلنا لعدة نتائج وتوصيات على النحو التالي:

أولاً: النتائج.

١) إن التحقيق في جرائم امن الدولة المعلوماتي له خصوصية يتميز بها عن التحقيق التقليدي، ويكتسب هذه الخصوصية من حيث طبيعة جرائم أمن الدولة المعلوماتي التي نص عليها المشرع الإماراتي في مرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ بشأن مكافحة جرائم الشائعات والجرائم الإلكترونية، كما ان خصوصية التحقيق في جرائم أمن الدولة المعلوماتي تظهر من خلال طبيعة الوسائل التي يستخدمها مرتكب الجريمة من حيث اعتماده على الوسائل المعلوماتية الحديثة، كما أن مرتكب جرائم أمن الدولة المعلوماتي يوصف بأنه من طائفة المجرمين من ذوي الخبرة الكبيرة في التقنيات الحديثة.

٢) لقد استحدث المشرع الإماراتي نيابة اتحادية خاصة بجرائم امن الدولة المعلوماتي وفق قرار وزير العدل، وهذه النيابة متخصصة بالتحقيق في جرائم أمن الدولة المعلوماتي التي نص عليها المشرع الإماراتي في قانون مكافحة الشائعات والجرائم الإلكترونية، دون أن يمتد اختصاصها لجرائم أمن الدولة الأخرى التي نص عليها قانون الجرائم والعقوبات الاتحادي، التي تختص بالتحقيق بها نيابة أمن الدولة.

٣) إن من أبرز التحديات التي تواجه جهة التحقيق في جرائم أمن الدولة، قدرة مرتكب الجريمة على استخدام التقنيات الحديثة بشكل فائق كما أنه قادر على تدمير الأدلة بشكل واسع وحرفي كبير، كما أن مسألة الحصول على الأدلة الإلكترونية في جرائم أمن الدولة المعلوماتي تشكل تحدياً كبيراً لدى جهات التحقيق.

ثانياً: التوصيات

نوصى المشرع الإتحادى الإماراتي بالتالى.

١) إضافة مواد قانونية لقانون الإجراءات الجزائية الاتحادي الصادر بمرسوم بقانون اتحادي رقم (٣٨) لسنة ٢٠٢٢ تنظم تكوين نيابة أمن الدولة، والنيابة الاتحادية لمكافحة جرائم الشائعات والجرائم الإلكترونية، في الفصل الخاص بتنظيم عمل النيابة العامة.

٢) تحديد اختصاصات نيابة أمن الدولة والنيابة الاتحادية لمكافحة جرائم الشائعات والجرائم الإلكترونية في التحقيق وبيان خصوصية التحقيق في هذا النوع من الجرائم ابتعاداً عن السياق العام لتنظيم إجراءات التحقيق في الجرائم التقليدية.

٣) إدراج مواد خاصة تتعلق بوسيلة ارتكاب الجرائم الماسة بأمن الدولة من جهة الخارج باستخدام التقنيات الحديثة في قانون مكافحة الشائعات والجرائم الإلكترونية وآلية التحقيق فيها وفق لكل وسيلة من هذه الوسائل، حيث تبين هذه المواد بشكل واضح وسائل ارتكاب الجرائم الماسة بأمن الدولة من جهة الخارج باستخدام التقنيات الحديثة.

٤) سن قوانين إجرائية تساعد على تنفيذ وتطبيق قوانين مكافحة الشائعات والجرائم الإلكترونية أو على الأقل تعديل القوانين الإجرائية السارية بشكل يستوعب التطورات الحاصلة في مجال تقنية المعلومات.

٥) إبرام المزيد من الاتفاقيات الأمنية مع الدول على المستوى الإقليمي والدولي وذلك من أجل التعاون الأمني لمواجهة الجرائم الماسة بأمن الدولة من جهة الخارج والتي تستخدم فيها التقنيات الحديثة.

قائمة المراجع

اولاً: الكتب العامة

١) ابن المنظور، أبو الفضل جمال الدين، **"لسان العرب "**، المجلد الأول، دار صادر للطباعة والنشر، بيروت ٢٠٠٠

٢) أيمن ناصر بن حمد العباد: المسؤولية الجنائية لمستخدمي شبكات التواصل الاجتماعي، مكتبة القانون والاقتصاد، الرياض، ط١، ٢٠١٦

٣) إيهاب عبد المطلب: جرائم الإرهاب داخلياً وخارجياً في ضوء القضاء والفقه، المركز القومي للإصدارات القانونية، القاهرة، ط١،٢٠٠٩م

٤) جميل زكريا، الأمن والانترنت، ورقة عمل مقدمة بندوة الأمن والإنترنت، أكاديمية الشركة (مركز بحوث الشرطة)، القاهرة، ٢٠٠٣/٦/١٥.

٥) جوده حسين جهاد : شرح قانون الإجراءات الجزائية الاتحادي، أكاديمية شرطة دبي، دبي، ٢٠١٦

٦) حسني الجندي: التشريعات الجنائية الخاصة في دولة الإمارات العربية المتحدة، الكتاب الثالث، بدون دار نشر، ط١، ٢٠٠٩م،

٧) خالد حسن أحمد لطفي : جرائم الإنترنت ـــ دار الفكر الجامعي – الإسكندرية – مصر – الطبعة الأولى – ٢٠١٨م

٨) خالد عياد الحلبي: جرائم الإنترنت، دار النهضة العربية، القاهرة، ٢٠١٨،

٩) خالد ممدوح إبراهيم: الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، ٢٠٠٩

١٠) راشد بشير ابراهيم: الجرائم الإلكترونية، دار وائل، عمان، ٢٠١٩،

١١) سليمان أحمد فضل: المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الإنترنت)، دار النهضة العربية، سنة ٢٠١٣

١٢) ضرغام جابر عطوش آل مواش: جريمة التجسس المعلوماتي، المركز العربي للنشر، مكتبة دار السلام القانونية، القاهرة، ٢٠١٦

١٣) محمد شلال العاني و الاستاذ الدكتور عبدالإله محمد النوايسة: شرح قانون الإجراءات الجزائية الإماراتي في ضوء المرسوم بقانون اتحادي رقم (٣٨) لسنة ٢٠٢٢ ، دار النهضة العربية، القاهرة، ٢٠٢٣

١٤) محمد عبد الله أبو بكر: جرائم الكمبيوتر والإنترنت، منشأة المعارف،الإسكندرية، ٢٠٠٦

١٥) محمد علي سويلم : مكافحة الجرائم الإلكترونية ـــ دار المطبوعات الجامعية – القاهرة – مصر – الطبعة الأولى – ٢٠١٩م

١٦) محمد مراد عبد الله: شبكات التواصل الاجتماعي ودورها في نشر الأفكار الهدامة، بحوث ودراسات شرطية، مركز دعم اتخاذ القرار، شرطة دبي، العدد (٢٦٤) ديسمبر ٢٠١٨

١٧) محمود نجيب حسني: الإجراءات الجزائية، دار النهضة العربية، القاهرة، ١٩٩٩،

١٨) هالة أحمد الرشيدي : الإرهاب السيبراني ـــ دار النهضة العربية – القاهرة – مصر – الطبعة الأولى – ٢٠٢١م

١٩) هشام فريد رستم قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الكاتبة، ١٩٩٥م

ثانياً: الكتب المتخصصة

١) أسامة أحمد المناع*سة والقاضي جلال محمد الزعبي : جرائم تقنية نظم المعلومات الإلكترونية ـــ دار الثقافة للنشر والتوزيع – عمان - الأردن – الطبعة الرابعة – ٢٠٢٢م

٢) أمير فرج يوسف: جرائم أمن الدولة العليا في الداخل والخارج، دار المطبوعات الجامعية، الإسكندرية، ٢٠٠٩م
٣) الجبالي منصور بن عبد العزيز، "مبادئ التحقيق الجنائي"، مكتبة فهد الوطنية، الطبعة الأولى ٢٠٠٨،
٤) خالد سامي السيد : الأمن القومي الإلكتروني وجرائم المعلومات– دار النهضة العربية – القاهرة – مصر – الطبعة الأولى – ٢٠٢١
٥) خالد سامي السيد : الأمن القومي الإلكتروني وجرائم المعلومات– دار النهضة العربية – القاهرة – مصر – الطبعة الأولى – ٢٠٢١
٦) راشد محمد المري : الجرائم الإلكترونية في ظل الفكر الجنائي المعاصر– دار النهضة العربية للنشر والتوزيع – القاهرة – مصر – الطبعة الأولى – ٢٠١٨م
٧) سمير عالية: الوجيز في شرح الجرائم الواقعة على أمن الدولة، المؤسسة الجامعية للدراسات والنشر والتوزيع، ط١، بيروت، ١٩٩٩م،
٨) عبد الفتاح حجازي: القانون الجنائي والتزوير في جرائم الحاسوب والانترنت، دار الكتب القانونية، مصر، ٢٠٠٥م، ص٢٤.
٩) عبد الله ذيب محمود والدكتور أسامة إسماعيل دراج : الوجيز في الجرائم الإلكترونية ـــ دار الثقافة للنشر والتوزيع – عمان – الأردن - الطبعة الأولى – ٢٠٢٢م
١٠) عماد مجدي عبد الملك: جرائم الكمبيوتر والانترنت، دار المطبوعات الجامعية، ٢٠١١م،
١١) محمد سعيد العامري : الأمن السيبراني والتحقيقات الرقمية ـــ المطبعة المتحدة للطباعة والنشر – أبو ظبي – الإمارات العربية المتحدة – الطبعة الأولى – ٢٠٢١م
١٢) محمد عبيد الكعبي: الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت، دار النهضة العربية، القاهرة، ٢٠٠٥م
١٣) محمود سليمان موسى: الجرائم الواقعة على أمن الدولة، دار المطبوعات الجامعية، الإسكندرية، ٢٠٠٩م

ثالثاً: الرسائل العلمية

١) حسن البلوشي: الجرائم الواقعة على أمن الدولة الداخلي باستخدام شبكة الإنترنت، رسالة ماجستير، أكاديمية شرطة دبي، دبي، ٢٠١٧
٢) حنان محمد الحسيني أحمد، وسحر علي عبدالله الهبدان. "التحقيق الجنائي الرقمي". مجلة جامعة الملك سعود - الحقوق والعلوم السياسية مج ٣٣، ع٢، (٢٠٢١):
٣) السويدي، أحمد غانم سيف (٢٠١٦). المواجهة الجنائية والأمنية للجرائم الماسة بأمن الدولة الداخلي دبي: أكاديمية شرطة دبي، كلية الدراسات العليا.
٤) عبد الله بن حسين الجراف القحطاني، **"تطوير مهارات التحقيق الجنائي في مواجهة الجريمة المعلوماتية "**، رسالة مقدمة لنيل شهادة الماجستير، قسم العلوم الشرطية، جامعة نايف للعلوم الأمنية، الرياض ٢٠١٤،
٥) نداء المصري: خصوصية الإثبات في الجرائم المعلوماتية، رسالة ماجستير، جامعة النجاح الوطنية، نابلس، ٢٠٠٧م
٦) ياسر الكتبي: جريمة الإتلاف الإلكتروني في قوانين دول مجلس التعاون لدول الخليج العربية أطروحة ماجستير لاستكمال متطلبات الحصول على درجة الماجستير في القانون العام، جامعة عجمان، ٢٠٢٣.

رابعاً: البحوث والمقالات

١) أيسر محمد الجرائم عطية: المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، المتلقي العامي، ورقة علمية بعنوان: دور الآليات الحديثة للحد من الجرائم المستحدثة، الإرهاب الإلكتروني وطرق مواجهته، كلية العلوم الاستراتيجية، الأردن، ٢٠١٩
٢) بين جيتس: "المعلوماتية بعد الإنترنت طريق المستقبل" - ترجمة أ. عبد السلام رضوان، إصدار المجلس الوطني للثقافة والفنون والأدب، الكويت، سلسلة عالم المعرفة – ٢٠١٤، العدد ٢٣١،
٣) حنان محمد الحسيني، وسحر علي عبدالله الهبدان. "التحقيق الجنائي الرقمي". مجلة جامعة الملك سعود - الحقوق والعلوم السياسية مج ٣٣، ع٢، (٢٠٢١):

٤) دراسة شاملة عن الجريمة السيبرانية، فيينا: مكتب الأمم المتحدة المعني بالمخدرات والجريمة، فبراير ٢٠١٣م،

٥) ضاحي خلفان تميم: الإنترنت رؤية امنية، بحوث ودراسات شرطية، مركز البحوث والدراسات، القيادة العامة لشرطة دبي، العدد (٥٧)، سبتمبر ١٩٩٦، ص ٢.

٦) عبد الله بن عبد العزيز العجلان: الرهاب الإلكتروني في عصر المعلومات، بحث متقدم إلى المؤتمر الدولي الأولحول "حماية أمن المعلومات والخصوصية في قانون الإنترنت"، والمنعقد بالقاهرة في المدة من ٢-٤ يونيو ٢٠٠٨م.

٧) عبد الناصر محمد فرغلي، ومحمد عبيد المسماري: بحث بعنوان الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية مقدم للمؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، جامعة نايف للعلوم الأمنية، الرياض، في الفترة ما بين ٢-١٤٢٨/١١/٤،

خامساً: القوانين

١) دولة الإمارات العربية المتحدة - قرار وزير العدل - رقم ٥٥٧ لسنة ٢٠٠٩ الصادر بتاريخ ٢٠٠٩-٠٧-١٦ نشر بتاريخ ٢٠٠٩-٠٧-٣٠ يعمل به إعتبارا من ٢٠٠٩-٠٧-٣٠ بشأن الهيكل التنظيمي للنيابة العامة الاتحادية. الجريدة الرسمية ٤٩٦ السنة التاسعة والثلاثون

٢) دولة الإمارات العربية المتحدة - مرسوم بقانون اتحادي - رقم ٣٤ لسنة ٢٠٢١ الصادر بتاريخ ٢٠٢١-٠٩-٢٠ نشر بتاريخ ٢٠٢١-٠٩-٢٦ يعمل به إعتبارا من ٢٠٢٢-٠١-٠٢ بشأن مكافحة الشائعات والجرائم الإلكترونية. الجريدة الرسمية ٧١٢ ملحق - السنة الواحد والخمسون

سادساً: احكام القضاء

١) المحكمة الاتحادية العليا - الأحكام الجزائية - الطعن رقم ٢٣٩ -لسنة ٢٠١٣ قضائية - تاريخ الجلسة ٢٠١٣-١١-١٢

٢) المحكمة الإتحادية العليا - الأحكام الجزائية - الطعن رقم ١٩٦ لسنة ٣٠ قضائية بتاريخ ٢٠٠٢-١١-٢٥ [رفض]

٣) المحكمة الإتحادية العليا - الأحكام الجزائية - الطعن رقم ١١٣ لسنة ٣٣ قضائية بتاريخ ٢٠٠٥-٠٦-٠٦ [تصحيح الحكم]

٤) محكمــة التمييــز - الأحكــام الجزائيــة – الطعــن رقــم ٢١٧ – لســنة ٢٠٠٣ قضــائية – تــاريخ الجلسة ٢٠٠٣-١٠-١٨ – مكتب فني ١٤ – رقم الجزء ١ – رقم الصفحة ٢٤٩

سابعاً: المراجع الأجنبية

Rosenblatt. K. S. High-Technology Crime: Investigating Cases Involving Computer. San Jose: KSK Publications. 1999,

ثامناً: الروابط الإلكترونية

1) https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Study_Arabic.pdf .
2) www.arablawinfo.com/Researches_AR/126.doc .

(37)

(48)

https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Study_Arabic.pdf .