Vol. 2, No. 1, pp. 365-396 | 2024
CFORSJ Procedia

المواجهة الأمنية والتعاون الدولي لدولة الإمارات العربية المتحدة لجريمة السب باستخدام الوسائل الإلكترونية

SECURITY CONFRONTATION AND INTERNATIONAL COOPERATION OF THE UNITED ARAB EMIRATES TO THE CRIME OF INSULT USING ELECTRONIC MEANS

[i*] Mohamed Haji Mohamed Siddiq Aljasmi, [ii] Wan Abdul Fattah Bin Wan Ismail & [iii] Dina Binti Imam Supaat

[i, ii, iii] Faculty of Syariah and Law, Universiti Sains Islam Malaysia, Bandar Baru Nilai

*(Corresponding author) e-mail: moh.m88m@gmail.com

ABSTRACT

Crimes committed via electronic means raise many issues related to arresting and bringing in accused persons, unless the behaviors are such as terrorism crimes, crimes against state security, crimes against intellectual property rights, drug and weapons crimes, and juvenile prostitution. The rest of the types of electronic crimes are often considered, in terms of the procedures followed in pursuing and arresting the perpetrators, as traditional crimes. In other words, the same procedures followed in pursuing and arresting the perpetrators of traditional crimes are applied to them, especially since there is a difference in the concept of some crimes. The procedures for collecting evidence are among the criminal litigation procedures, but rather they are a stage prior to the investigation and trial procedures and pave the way for them. This stage aims to uncover crimes that have actually occurred with the aim of reaching the perpetrator and bringing him to trial. These procedures fall, according to the original jurisdiction of judicial police officers. It is necessary to take into account the objective and formal rules and conditions when conducting an inspection in cybercrimes, including the crimes of defamation, in order to achieve the balance that the criminal legislator is keen on, as violating these conditions and rules results in the invalidity of the inspection procedures and the resulting effects. Security cooperation at the Arab level in combating cybercrimes is a basic and necessary requirement, as the internal and external security of each Arab country is linked to collective Arab security, and the disruption of internal security in any country necessarily extends to disrupting stability in all aspects of life, which ultimately affects the outcome of the self-power of all Arab countries. Accordingly, each Arab country must commit to adopting the necessary measures to implement the obligations contained in the agreement, and provide the necessary security assistance and communications to combat information technology crimes.

Keywords: *Confrontation, Security, Crime of Insult, Electronic Means*

ملخص البحث

تثير الجرائم المرتكبة عبر الوسائل الإلكترونية العديد من الأشكال المتعلقة بضبط وإحضار المتهمين ما لم تكن السلوكيات من قبيل جرائم الإرهاب أو الجرائم الماسة بأمن الدولة، أو الجرائم الماسة بحقوق الملكية الفكرية وجرائم المخدرات والأسلحة وإباحة الأحداث، إذ أنه غالباً ما يتم اعتبار بقية أنماط الجرائم الإلكترونية من حيث الإجراءات المتبعة في ملاحقة وضبط الجناة من قبيل الجرائم التقليدية، بمعني آخر تطبق بشأنها ذات الإجراءات المتبعة في ملاحقة وضبط الجناة مرتكبي الجرائم التقليدية، لاسيما وأن هناك اختلاف في مفهوم بعض الجرائم وإن إجراءات جمع الاستدلالات من إجراءات الخصومة الجزائية، بل هي مرحلة سابقة على إجراءات التحقيق والمحاكمة وتمهد لهما، وتهدف هذه المرحلة إلى الكشف عن الجرائم التي وقعت بالفعل بهدف التوصل إلى مرتكبها وتقدمه للمحاكمة، وتدخل هذه الإجراءات بحسب الأصل في الاختصاص الأصيل لمأموري الضبط القضائي. ومن الضروري مراعاة القواعد والشروط الموضوعية والشكلية عند إجراء التفتيش في الجرائم الإلكترونية، ومنها جريمتي السب، وذلك حتى تتحقق الموازنة التي يحرص عليها المشرع الجزائي، إذ أن مخالفة هذه الشروط والقواعد يترتب عليها بطلان إجراءات التفتيش وما ينتج عنها من آثار. ويعد التعاون الأمني على المستوى العربي في مكافحة الجرائم الإلكترونية مطلب أساسي وضروري، حيث أن الأمن الداخلي والخارجي لكل دولة عربية مرتبط بالأمن العربي الجماعي، وأن الإخلال بالأمن الداخلي في أي دولة تتعدى آثاره بالضرورة إلى الإخلال بالاستقرار في كافة نواحي الحياة، مما يؤثر في النهاية على محصلة القوة الذاتية للدول العربية كافة، وعليه يجب أن تلتزم كل دولة عربية بتبني الإجراءات الضرورية من أجل تطبيق الالتزامات الواردة في الاتفاقية، وتقديم المساعدة والاتصالات الأمنية اللازمة لمكافحة جرائم تقنية المعلومات.

الكلمات المفتاحية: *المواجهة، الأمنية، جريمة السب، الوسائل الإلكترونية*

مقدمة

اتفق علماء الإجرام على أن الجريمة ظاهرة اجتماعية، تتأثر حجماً واتجاهاً وصوراً وأنماطاً بالمتغيرات المختلفة على كافة مستوياتها الاقتصادية والاجتماعية والثقافية، ولا شك أن المجتمع الدولي يمر في الوقت الراهن بثورة هائلة من التحولات بما يعرف اصطلاحاً بظاهرة العولمة والاتصالات، والتي أفرزت حالة من التواصل الإنساني بفضل الثورة المعلوماتية، والتي عكست أنساقاً قيمية وثقافية ذات مردودات سلبية صاحبها ظهور أنماط إجرامية مستحدثة

اتخذت من الشبكة المعلوماتية ووسائل تقنية المعلومات أداة ووسيلة ومحلاً للاعتداء على المصالح والقيم الاجتماعية والشخصية[1].

تتسم جرائم تقنية المعلومات بصعوبة اكتشافها وإثباتها، ويرجع ذلك إلى خصائص تقنية المعلومات ذاتها، وخاصة السرعة العالية التي ترتكب بها، وهو ما يسهل ارتكابها ويسهل طمس معالمها ومحو آثارها قبل اكتشافها، إذ يستطيع الجاني أن يرتكب الجريمة دون أن يترك وراءه أي أثر خارجي ملموس، وإذا كانت ثمة دليل على الإدانة فيستطيع الجاني تدميره في ثوانٍ معدودة، خاصة وأن هذا النوع من الجرائم يعتمد على الذكاء في ارتكابها، وأن المجرم المعلوماتي يتميز بالمهارة التقنية العالية والمعارف الفنية في مجال المعلوماتية وأنظمة وبرامج الحاسبات.

وتعتبر الجريمة المعلوماتية شكلاً جديداً من أشكال الجرائم العابرة للحدود الدولية بين كافة الدول، أي أنه يمكن عن طريق شبكة الإنترنت ارتكاب العديد من الجرائم وبخاصة الجرائم التي تمس الحق في الخصوصية ومنها جريمة التشهير الإلكتروني، وإذا كانت هناك جريمة واضحة تستحق التحقيق بالفعل، فإنه قد يكون هناك حاجة إلى مساعدة من البلد الذي كان منشأ الجريمة أو من سلطات الدول التي عبر من خلالها النشاط المجرَم، أو حيث توجد أدلة الجريمة، وكل ذلك يتطلب نوعاً من التعاون الدولي بين مختلف الدول لردع ذلك النوع من الجرائم[2].

وقد تزامن الحديث عن الجرائم الإلكترونية في الفترة الأخيرة مع بروز مجموعة من الظواهر والمستجدات الفكرية والتطورات التكنولوجية والعلمية، التي تتجه نحو زيادة ترابط العالم وتقاربه، مما أدى إلى فتح الحدود بين الأفراد والمجتمعات والثقافات والدول، كما أضحى من الصعوبة بمكان الاستغناء عن الخدمات والفوائد العظيمة التي تقدمها الثورة التكنولوجية، إلا أن النفس البشرية قد تميل أحياناً إلى فعل أشياء مخالفة للقوانين، حيث يستغل بعض الأفراد المكتشفات العلمية وما تقدمه من وسائل وأدوات تكنولوجية متقدمة في ارتكاب العديد من الجرائم التقليدية مستغلين الإمكانيات الهائلة لهذه الاختراعات الحديثة، أو استحداث صور إجرامية أخرى ترتبط بهذه التقنيات الحديثة[3].

ويلاحظ أن الجريمة الإلكترونية المرتكبة عبر الوسائل الإلكترونية أو أي وسيلة من وسائل تقنية المعلومات لا تختلف عن الجريمة التقليدية، نظراً لأنها تخالف القانون، وتعتبر تعدي على حقوق الغير في شخصه وممتلكاته، لاسيما ما يتعلق منها بسمعة الإنسان ومكانته واعتباره في المجتمع، وعلى وجه الخصوص السب ، والتي تعد أحد أنواع الجرائم المعلوماتية التي أرقّت مستخدمي التقنيات الحديثة[4]، إذ أصبح البعض يستخدم أدوات التقنيات الحديثة ووسائل التواصل الاجتماعي في سب وقذف الغير أو خدش شرفه أو اعتباره[5]، الأمر الذي حدا بالكثير من

1 محمد البشرى، محمد الهنائي، الجرائم الإلكترونية وسبل مواجهتها، مركز البحوث الأمنية، أبوظبي، 2009، ص 19.

2 علاء الدين شحاتة، التعاون الدولي في مجال مكافحة الجريمة، دار النهضة العربية، القاهرة، 2007، ص 174.

3 هشام محمد فريد، الجرائم المعلوماتية وطرق مواجهتها، مركز بحوث الشرطة، القاهرة، 2015، ص 21.

4 سالم روضان الموسوي، جرائم القذف والسب عبر القنوات الفضائية، منشورات الحلبي، بيروت، 2012، ص 33.

5 دينا عبد العزيز، الحماية الجنائية من إساءة استخدام مواقع التواصل الاجتماعي، دراسة مقارنة، دار النهضة العربية، القاهرة، 2018م، ص73.

الدول إلى إصدار تشريعات جزائية خاصة لمكافحة الجرائم الإلكترونية نصت فيها على تجريم السب ، حيث نجد أن المشرع الإماراتي سعى إلى وضع تشريع استشرافي يمكن من خلاله قياس الأثر التشريعي له عن طريق تقييم مدى ملائمته وانسجامه مع التطور التكنولوجي في وسائل تقنية المعلومات الذي تحياه الدولة من جانب، وتعزيز الشعور بالأمن والأمان من جانب آخر[6].

فدولة الإمارات العربية المتحدة من الدول المتقدمة في المجال المعلوماتي والتكنولوجي، وكانت من أوائل الدول العربية[7] التي تنبهت إلى خطر الجريمة المعلوماتية، وسنت قوانين ملزمة بشأنها لمعاقبة من يتسبب في الإساءة إلى شخص آخر عبر الوسائل الإلكترونية، لاسيما جرائم السب، كونها من الجرائم التي لها الأثر البالغ سلباً على شخص الإنسان، ومن الجرائم الأكثر شيوعاً في المجتمع، وفي هذا الإطار وفرت الجهات الأمنية كافة الجهود التكنولوجية للتبليغ عن هذه الجرائم المعلوماتية ضمن إجراءات وآليات مكافحة أمنية متطورة.

مشكلة البحث

تعد التقنية الحديثة التي أصبحت متيسرة في كثير من الدول وتعد من العوامل المساعدة على القيام بمثل هذا النشاط الإجرامي المستحدث، حيث تأثرت بالاشتراك المتسارع والدخول في شبكة الإنترنت بنسبة عالية وتعد جريمة السب المرتكبة عبر الوسائل الإلكترونية من أكثر الجرائم الماسة بالشرف والسمعة والاعتبار والاعتداء على خصوصية الآخرين وانتهاكها، فقد يؤدي السب بالآخرين عبر الشبكة المعلوماتية إلى حدوث مشكلات تؤثر على الوضع النفسي للشخص الذي يتم سبه أو قذفه، وخاصة في مجتمعاتنا العربية، وبسبب عاداتنا وتقاليدنا.

وعليه تتمثل مشكلة البحث في إن الجرائم المعلوماتية هي أي نشاط غير قانوني أو غير أخلاقي يتم من خلال استخدام الإنترنت أو الحاسوب كأداة لجريمة إلكترونية تنتهك بيانات الأفراد أو الكيانات الدولية، ويحاول مجرمو الإنترنت استغلال البرامج الإلكترونية في اختراق بيانات المستخدمين والوصول إلى المعلومات الشخصية أو أسرار الأعمال التجارية أو استخدام الإنترنت لأغراض استغلالية أو ضارة بالأفراد، ويمكن لمجرمي الإنترنت أيضًا استخدام أجهزة الحاسوب للاتصال وتخزين المستندات، وغالبًا ما يُشار إلى المجرمين الذين يقومون بهذه الأنشطة غير القانونية على أنهم مُخترقون، من خلال توضيح ما مدى كفاية الإجراءات التشريعية والأمنية للحد من جريمة

6 عبيد صالح حسن، سياسة المشرع الإماراتي لمواجهة الجرائم الإلكترونية، مجلة الفكر الشرطي، مركز بحوث الشرطة، الشارقة، العدد 95، أكتوبر 2015م، ص 38.

7 أدرك المشرع الإماراتي أهمية وضع تشريع خاص لمكافحة الجرائم الإلكترونية ووضع عقوبات رادعة لتحقيق أهداف العقوبة وهو القانون الاتحادي رقم (2) لسنة 2006 بشأن مكافحة جرائم تقنية المعلومات، والذي استمد نصوصه من قانون العقوبات الاتحادي، إلا أنه مع اختلاف في الوسيلة المرتكبة للجريمة، فقد أثبت الواقع العملي قصور هذا التشريع وعدم قدرته على مواكبة التطورات السريعة والمخاطر التي نتجت عن التقدم المذهل في وسائل تقنية المعلومات وظهور أنواع جديدة من الجرائم التي لم يتعرض لها هذا التشريع، وبالتالي دعت الحاجة إلى النص على جرائم حديثة وتشديد العقوبات وتوسيع نطاق تطبيق بعضها، لتواكب وتغطي ما لم يكن متناولاً أثناء صدور التشريع القديم، وهو الأمر الذي دفع المشرع إلى إلغائه واستبداله بالمرسوم بقانون اتحادي رقم (5) لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات وتعديلاته، والذي تم إلغاؤه بموجب المرسوم بقانون اتحادي رقم (34) لسنة 2021 بشأن مكافحة الشائعات والجرائم الإلكترونية.

السب المرتكبة عبر الوسائل الإلكترونية، وماهية التعاون الأمني على المستوى الدولي في مجال مكافحة الجرائم المعلوماتية.

أسئلة البحث

ستقوم هذه الدراسة بالإجابة على الأسئلة الأتية:

1. ما هي إجراءات تلقي البلاغات في جرائم السب المعلوماتي؟
2. ما هي إجراءات المعاينة وضبط الأشياء والتفتيش في جرائم السب المعلوماتي؟
3. ما هو دور التعاون الأمني على المستوى الدولي في مجال مكافحة الجرائم المعلوماتية؟
4. ما هي أليات تسليم المجرمين في مجال الجرائم المعلوماتية؟

أهداف البحث

ستقوم هذه الدّراسة بالإجابة عن الأسئلة الآتي:

1) بيان إجراءات تلقي البلاغات في جرائم السب المعلوماتي.
2) التعرف على إجراءات المعاينة وضبط الأشياء والتفتيش في جرائم السب المعلوماتي.
3) بيان دور التعاون الأمني على المستوى الدولي في مجال مكافحة الجرائم المعلوماتية.
4) توضيح أليات تسليم المجرمين في مجال الجرائم المعلوماتية.

منهجية البحث

اعتمد هذا البحث على **المنهج الوصفي التحليلي**، وذلك من خلال تحليل مضمون النصوص القانونية ذات العلاقة بالمواجهة التشريعية والأمنية لجرائم السب وتوضيح إجراءات المعاينة وضبط الأشياء والتفتيش في جرائم السب المعلوماتي، من خلال المرسوم بقانون اتحادي رقم (31) لسنة 2021 بشأن الجرائم والعقوبات بقانون اتحادي رقم 38 لسنة 2022 بإصدار قانون الإجراءات الجزائية، وتوضيح دور التعاون الأمني على المستوى بالإضافة إلى الأحكام القضائية ذات العلاقة بموضوع البحث من أجل تقييم موقف المشرع الإماراتي من مكافحة جرائم السب عبر الوسائل الإلكترونية

الدراسة السابقة

1. وفي دراسة سابقة تم نشرها حول (الحماية الجنائية للبيانات الشخصية في مواجهة الجرائم الإلكترونية)[8]: هدفت هذه الدراسة إلى التعرف على الأساس القانوني لحماية البيانات الشخصية من مخاطر الإنترنت، وإبراز أهم صور الحماية الجنائية لحماية الحياة الشخصية عبر شبكة الإنترنت، وتوضيح العقوبات والتدابير المقررة للجرائم المترتبة على انتهاك الحق في خصوصية البيانات الشخصية عبر الوسائل الإلكترونية في التشريع الإماراتي والمقارن، وتوصلت الدراسة إلى أن المشرع الإماراتي أضفى على البيانات الشخصية حماية ومنع انتهكاها، وتقييد أنشطة جمعها ومعالجتها ونقلها واستخدامها على نحو يوفر حماية لحياة الأفراد الخاصة من مخاطر تقنية المعلومات واستخداماتها، وجرم تلك الأفعال لو تمت عبر وسائل تقنية المعلومات، وأوصت الدراسة بأن يكون الأمر بالإبعاد المنصوص عليه في المادة (42) من المرسوم بقانون اتحادي رقم (5) لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات وتعديلاته جوازياً للقاضي وتعطى له سلطة تقدير الحكم بالإبعاد أو الاكتفاء بالعقوبات الأصلية، لاسيما أن غالبية الجرائم المنصوص عليها في هذا المرسوم من نوعية الجنح.
2. وفي دراسة أخرى تم نشرها حول (السياسة العقابية للمشرع الإماراتي في مواجهة الجرائم المعلوماتية جرائم السب والقذف)[9]: هدفت هذه الدراسة إلى التعرف على فلسفة وتطور العقوبات المقررة على الجرائم المستحدثة عن طريق استخدام وسائل التقنية الحديثة وفقاً للمرسوم بقانون اتحادي رقم (5) لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات وتعديلاته، والبحث في فلسفة ونهج المشرع الإماراتي للعقوبات والتدابير الاحترازية التي قررها في تلك الجرائم، وتوصلت هذه الدراسة إلى عدة نتائج أهمها أن المشرع الإماراتي صنف العقوبات في جرائم تقنية المعلومات إلى عقوبات سالبة للحرية وعقوبات مالية مستندة إلى مبدأ الشرعية معتقداً أن في ذلك تحقيق الردع العام والخاص معاً، وتم النص على بعض

8 حسن محمد حسنوه الظنحان، الحماية الجنائية للبيانات الشخصية في مواجهة الجرائم الإلكترونية، دراسة مقارنة، رسالة ماجستير غير منشورة، كلية الإمام مالك للشريعة والقانون، دبي، 2020م.

9 عبد العزيز سالم السنيدي، السياسة العقابية للمشرع الإماراتي في مواجهة الجرائم المعلوماتية، رسالة ماجستير غير منشورة، كلية القانون، جامعة الإمارات العربية المتحدة، 2018م.

التدابير الاحترازية الجديدة في المرسوم غير محددة المدة، وأوصت الدراسة ببحث إمكانية تطبيق المراقبة الإلكترونية كأسلوب حديث للتدابير الاحترازية كبديل عن العقوبات السالبة للحرية قصيرة المدة.

3. وفي دراسة أخرى تم نشرها حول(جرائم الاعتبار عبر شبكة الإنترنت "جريمي السب والقذف")[10]: هدفت هذه الدراسة إلى توضيح كيفية ارتكاب جرائم الاعتبار عبر شبكة الإنترنت، لاسيما جرائم السب والقذف، وتسليط الضوء على المسؤولية الجنائية لمقدمي الخدمات الوسيطة في الإنترنت، واعتمدت هذه الدراسة على المنهج التحليلي المقارن، وتوصلت الدراسة إلى عدة نتائج أهمها أن جرائم القذف التي ترتكب عبر شبكة الإنترنت يتحقق فيها ركن العلانية، ويتعين أن يكون الجاني عالما بأن الواقعة التي يسندها إلى المجني عليه توجب عقابه أو احتقاره، كما توصلت إلى أن وجه الاختلاف بين السب والقذف يكمن في تحديد الواقعة المنسوبة للمجني عليه، فالقذف يتميز عن السب في أنه لا يتحقق إلا بإسناد واقعة معينة إلى المجني عليه، فإذا لم يحدد الجاني الواقعة التي تفيد هذا العيب اعتبر ما ارتكبه الجاني سباً، وأوصت الدراسة بتشديد العقوبات على جرائم السب والقذف الإلكترونية.

4. وفي دراسة أخرى تم نشرها خول (مكافحة جرائم السب والقذف عبر الإنترنت)[11]، هدفت هذه الدراسة إلى التعرف على مفهوم جرائم الإنترنت ومضمون جريمة السب والقذف، والتعرف على التكييف القانوني لكي من جريمتي السب والقذف، والتعرف على الشرعية القانونية والإجرائية لهاتين الجريمتين، ووسائل إثباتهما، وتوصلت الدراسة إلى عدة نتائج أهمها أنه على الرغم من هذا الكم الهائل من الجرائم التي ترتكب عبر شبكة الإنترنت، إلا أن هناك فراغ تشريعي في مواجهة هذه الجرائم ما زالت تخضع لقانون العقوبات العادي الذي أصبح غير قادر على مواجهة هذه النوعية من الجرائم المستحدثة التي تحتاج إلى تكييفها إلى قانون محدد، وعليه أوصت الدراسة إلى ضرورة أن يستحدث المشرع قوانين جديدة لمواجهتها وعدم اللجوء بشأنها إلى القواعد التقليدية.

5. وفي دراسة أخرى تم نشرها حول (دور التحريات والبحث الجنائي في الكشف عن الجرائم الإلكترونية)[12]: هدفت هذه الدراسة إلى التعرف على دور التحريات في الكشف عن الجرائم الإلكترونية، وتمثل مجتمع الدراسة في العاملين بإدارات التحريات والمباحث الجنائية بشرطة مكة المكرمة، ومن أهم النتائج التي توصلت إليها الدراسة موافقة أفراد الدراسة على أن دور التحريات في الكشف عن الجرائم الإلكترونية ضعيف، وموافقة أفراد الدراسة وبشدة على ضرورة وجود قدرات ومهارات تقنية لازمة للأفراد

---

10 أحمد سعد محمد الحسيني، جرائم الاعتبار عبر شبكة الإنترنت جريمتي السب والقذف"، مجلة البحوث القانونية والشرطية، أكاديمية الشرطة، القاهرة، العدد (9)، مارس 2018م.

11 عادل إبراهيم إسماعيل، مكافحة جرائم السب والقذف عبر الإنترنت، مجلة كلية الدراسات العليا، أكاديمية الشرطة، القاهرة، العدد 33، أكتوبر، 2015م.

12 سليمان العتيبي، دور التحريات والبحث الجنائي في الكشف عن الجرائم الإلكترونية، أطروحة دكتوراه غير منشورة، جامعة نايف العربية للعلوم الأمنية، الرياض، 2019م.

للكشف عن الجرائم الإلكترونية ووجود صعوبات تواجه التحريات والبحث الجنائي عند الكشف عن الجرائم الإلكترونية، وأوصت الدراسة بضرورة العمل على تأهيل وتدريب ضباط التحريات والمباحث الجنائية واستحداث وحدات تتعلق بالجريمة الإلكترونية.

أهمية البحث

1. الأهمية العلمية: يمكن أن تمثل الدراسة الراهنة إضافة علمية جديدة في مجال مكافحة الجرائم الإلكترونية خاصة في الدول التي تتسع فيها مجالات استخدام التكنولوجيا الحديثة مثل دولة الإمارات العربية المتحدة، وقد انعكس ذلك على المشرع الإماراتي في العقد الأخير نظراً لانتشار وتعدد وتنوع وسائل تقنية المعلومات في الدولة، ومن ثم لزم الأمر تأصيل علمي يوضح المواجهة الموضوعية الإجرائية (المواجهة الجزائية) لجريمة السب عبر الوسائل الإلكترونية، وذلك من خلال دراسة تأصيلية توضيحية الإجراءات الأمنية وكيفية المواجهة الأمنية والتعاون الدولي لدولة الإمارات العربية المتحدة للحد من جريمة السب المرتكبة عبر الوسائل الإلكترونية،
2. الأهمية العملية: تتجلى في تزايد اهتمام الدول خلال الفترة الحالية بموضوع جرائم تقنية المعلومات، واحتمالات حدوثها أصبح ظاهرة في ظل انتشار وسائل التكنولوجيا المتطورة، كما أن الواقع العملي أظهر استخدام المشرع الجزائي للأسلوب العقابي لمواجهة الكثير من الأنماط المستحدثة التي تتفاوت فيما بينها من حيث درجة جسامتها، وعيوب هذه السياسة المتمثلة ببروز ظاهرة تزايد أعداد الجرائم المرتكبة عبر وسائل تقنية المعلومات، وقد تساعد هذه الدراسة رجال البحث والتحري على تطوير مهاراتهم الأمنية للتعامل مع مرتكبي جرائم السب المرتكبة بواسطة الوسائل الإلكترونية، كما أن هناك حاجة ماسة للبحث المتعمق في المسائل العملية المتصلة بإجراءات الاستدلال والتفتيش لإثبات تلك الجرائم.

حدود البحث

1) الحدود الزمانية: تدور الحدود الزمانية في لدراسة المواجهة الأمنية والتعاون الدولي لدولة الإمارات العربية المتحدة لجريمة السب باستخدام الوسائل الإلكترونية خلال عام 2024 ومن خلال التواصل مع المشرف في وضع قواعد الدراسة وطرق إجرائها ومناقشة بعض الأمور في الدراسة وحتى تقديم هذه الدراسة.

2) الحدود المكانية: تتركز الحدود المكانية للدراسة في جمهورية ماليزيا بجامعة العلوم الإسلامية الماليزية وأيضاً من خلال الزيارات إلى وزارة الداخلية الإماراتية لإجراء بعض المقابلات مثال (شرطة دبي، وشرطة أبوظبي، وشرطة الشارقة) في كيفية الإجراءات والتعاون الدولي الذي يتم في مواجهة جرائم السب عبر الوسائل الإلكترونية.

المبحث الأول :إجراءات جمع الاستدلال في جرائم السب المعلوماتي

لا تعد إجراءات جمع الاستدلالات من إجراءات الخصومة الجزائية، بل هي مرحلة سابقة على إجراءات التحقيق والمحاكمة وتمهد لهما، وتهدف هذه المرحلة إلى الكشف عن الجرائم التي وقعت بالفعل بهدف التوصل إلى مرتكبها وتقدمه للمحاكمة، وتدخل هذه الإجراءات بحسب الأصل في الاختصاص الأصيل لمأموري الضبط القضائي[13]، وقد أشارت إلى ذلك المادة (30) من قانون الإجراءات الجزائية الإماراتي بقولها: "يقوم مأموري الضبط القضائي بتقصي الجرائم والبحث عن مرتكبيها وجمع المعلومات والأدلة اللازمة للتحقيق والإتهام".

وعليه فعندما تتضح معالم وقوع جريمة السب عبر الوسائل الإلكترونية، فإنه على مأموري الضبط القضائي المبادرة في الحال، ومن دون تباطؤ بالبحث والتحري عنها، وبمراقبة المشبوهين واستيقافهم وتعقب الجناة والبحث عنهم، وجمع الأدلة لإثبات إدانتهم.

ونظراً لتطبيق العديد من القوانين الإجرائية المتبعة في الجرائم العادية، فسوف نجد تكراراً لنفس القواعد الإجرائية المتبعة، نظراً لعدم صدور قواعد إجرائية خاصة بجرائم تقنية المعلومات[14]، إلا أنه ما يلاحظ من خلال الإطلاع على تجارب الجهات الشرطية في دولة الإمارات العربية المتحدة وجود اختلاف في تقديم البلاغ بجرائم تقنية المعلومات عن الجرائم التقليدية، كون جرائم السب التي ترتكب باستخدام الشبكة المعلومات تتمتع بالخصوصية.

وللتعرف على إجراءات جمع الاستدلال في جرائم السب المعلوماتي، سنقسم هذا المبحث على النحو الآتي:

المطلب الأول :إجراءات تلقي البلاغات في جرائم السب المعلوماتي

يبدأ مأموري الضبط القضائي بجمع الاستدلالات بعد تلقيهم البلاغات والشكاوى عن الجرائم، وغالباً ما يتم تقديم البلاغ أو الشكوى الجنائية المتعلقة بالجرائم الإلكترونية لمأموري الضبط القضائي في إدارات أو مراكز الشرطة بمنطقة الاختصاص، بيد أنه يمكن تقديمها للنيابة العامة مباشرة، فتقوم باتخاذ قرارها بشأن الموافقة أو الرفض على فتح بلاغ أو شكوى جنائية، فإن وافقت تأمر بإرسال الأوراق للجهة الشرطية المختصة، وذلك لجمع الأدلة الإلكترونية، واتخاذ ما يلزم من الكشف عن المتهم وسؤاله تمهيداً لإعادة الملف للنيابة العامة لتتخذ قراراها بالتصرف فيه[15].

---

13 خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الإسكندرية، 2010م، ص 31.

14 هلالي عبد اللاه أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية، دار النهضة العربية، القاهرة، 2007، ص 71.

15 محمد أحمد حبحب، جرائم تقنية المعلومات في دولة الإمارات، دار الكتاب الجامعي، العين، 2016م، ص 113.

ويقدم البلاغ بشأن الجرائم الإلكترونية إما **مادياً** وذلك بالتوجه لمأموري الضبط القضائي أو النيابة العامة بتقديم البلاغ شفاهة أو كتابة أو أن يقدم إلكترونياً من خلال الموقع الإلكتروني www.moi.gov.ae أو التطبيق الذكي لوزارة الداخلية UAE MOI[16]، أو أن يكون بلاغاً **معنوياً** وذلك في حالة إبلاغ الجهات الأمنية المختصة هاتفياً أو من خلال وسائل التواصل الاجتماعي نفسها، كما يمكن لمأمور الضبط القضائي التوصل للجريمة بنفسه من خلال وجود ما يسمى بالشرطة الإلكترونية وهم عبارة عن فريق من قسم الجرائم الإلكترونية بإدارة التحريات والمباحث الجنائية في القيادات الشرطية بالدولة، حيث يقوم برصد الجرائم المرتكبة عبر وسائل التواصل الاجتماعي ما لم تكن من جرائم الشكوى، خاصة ما إذا كان المحتوى متاحاً للعامة، إذ لا يتطلب الأمر الحصول على إذن من النيابة العامة لضبط هذه الجرائم[17].

هذا مع الأخذ بعين الاعتبار أن واجب مأموري الضبط القضائي بتلقي التبليغات والشكاوى يأتي متزامناً مع واجب أفراد المجتمع ممن علم منهم بوقوع جريمة التشهير الإلكتروني، إبلاغ السلطة المختصة عنها، سواء كانت جهة تلقي هذه التبليغات هي النيابة العامة أو مراكز الشرطة متمثلة في مأموري الضبط القضائي[18]، حيث نصت المادة (37) من قانون الإجراءات الجزائية الاتحادي على أن: (على كل من علم بوقوع جريمة مما يجوز للنيابة العامة رفع الدعوى عنها بغير شكوى أو طلب أن يبلغ النيابة العامة أو أحد مأموري الضبط القضائي عنها).

ويتمتع البلاغ في الجرائم الإلكترونية، ومنها جريمة السب عبر الوسائل الإلكترونية، بنوع من الخصوصية، نظراً للطبيعة الخاصة لهذه الجرائم، ويتحقق بمجرد تلقي مأمور الضبط القضائي بلاغاً يشير إلى قيام شخص بارتكاب جريمة سب أو قذف إلكتروني ضد آخر، وعلى الرغم من أن لكل فئة من جرائم المعلوماتية أسئلة معينة تختص بها، **إلا أنه هناك عدد من الأسئلة التي تعتبر ذات طبيعة مشتركة في غالبية تلك الجرائم تتناول جوانب محددة منها ما يأتي[19]:**

- تاريخ ووقت تلقي البلاغ.
- المعلومات الخاصة بالمبلغ.

---

16 مع إطلاق وزارة الداخلية بدولة الإمارات العربية المتحدة للتطبيق الذكي (مركز الشرطة في هاتفك) في بداية شهر أكتوبر 2018 فإنه بإمكان جميع أفراد المجتمع إنهاء كافة المعاملات الخاصة بمراكز الشرطة بسهولة وبطريقة ميسرة، وتقديم معاملاتهم وبلاغاتهم عبر التطبيق الذكي للوزارة (MOI-UAE) وذلك من أي مكان يتواجدون فيه، وبصرف النظر عن موقعهم الجغرافي. حيث يوفر التطبيق ميزة تقديم خدمات التبليغ والشكاوى الجنائية بطريقة سهلة وسريعة ويراعى فيها كافة الاحتياطات الأمنية وسرية المعلومات الشخصية لمقدم البلاغ، وذلك ضمن الإجراءات والضوابط القانونية. أنظر: "الداخلية تطلق مركز الشرطة في هاتفك"، مقال منشور في جريدة الاتحاد بتاريخ 2018/10/1 على الرابط: www.alittihad.ae/article/66533/2018 – تاريخ زيارة الموقع: 2024/7/05.

17 ياسر محمد الكومي، دور مرحلة جمع الاستدلالات في الحد من الجرائم المعلوماتية، مجلة البحوث القانونية والشرطية، أكاديمية الشرطة، القاهرة، السنة الرابعة، العدد السابع، مارس 2016، ص 138.

18 خالد حامد مصطفى، شرح قانون الإجراءات الجزائية لدولة الإمارات العربية المتحدة، دار الفكر والقانون، القاهرة، 2017، ص 119.

19 آمنة محمدي بوزينة، إجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية، مجلة الدراسات القانونية، كلية الحقوق والعلوم السياسية، جامعة حسيبة بوعلي، الجزائر، المجلد 6، العدد 14، يونيو 2017م، ص 19.

- المعلومات الخاصة بمتلقي البلاغ.
- طبيعة ونوع الجريمة المعلوماتية محل البلاغ.
- الأسئلة الستة الطبيعية في كل بلاغ (متى؟ وأين؟ وماذا؟ وكيف؟ ولماذا؟ ومن؟).
- المعلومات المتعلقة بالحاسوب أو الموقع الإلكتروني، وكيفية الاتصال بالجناة.

ويجب على رجل الشرطة أن يكون على يقين بأن عملية تلقي البلاغ لا تزيد عن كونها مجرد عملية مبدئية الغرض الأساسي منها هو تكوين صورة مبدئية عن كيفية وقوع تلك الجريمة، ومدى الخسائر أو التهديدات الناتجة عنها، وليس الغرض منها معرفة كافة الجوانب الفنية والقانونية للجريمة، وأن يكون لديه قناعة أن المجني عليه قد لا يستطيع الإجابة على كافة الأسئلة التي تدور في ذهنه، ولكن عليه فقط العلم بأن عملية تلقي البلاغ مجرد تحفيز لقدراته الذهنية، وخلق نوع من التفكير الإيجابي نحو الوصول إلى ظروف وملابسات ارتكاب الجريمة لضبط الجاني[20].

وبعد الانتهاء من المعلومات اللازمة من خلال سؤال المجني عليه أو الشخص المبلغ أو الاستفسار من أي مصادر أخرى محتملة، يبدأ رجال البحث والتحري، وعلى ضوء المعلومات التي توافرت لديه، في تحديد خطة العمل المناسبة وفريق العمل اللازم للتحقيق في الواقعة، وهذه الخطة يجب أن تكون قد اكتملت في ذهن المحقق بمجرد انتهائه من معاينة موقع ارتكاب الجريمة، واتضحت لديه الصورة الأولية عنها بإطلاعه على بعض الأمور الفنية والتقنية التي قد لا يكون الشخص المبلغ أطلعه عليها، ومما لا شك فيه أنه لو كان لدى المحقق خطة جيدة وفريق عمل تقني جاهز لتنفيذها فإن التعامل معها سيكون أسهل بكثير، والآثار السلبية الناتجة عنها أقل بكثير[21].

وفيما يلي نستعرض تجارب الأجهزة الشرطية بدولة الإمارات في التعامل مع الجرائم الإلكترونية:

2). تجربة القيادة العامة لشرطة الشارقة[22]

يقوم فرع جرائم التقنية بقسم الجريمة المنظمة التابع لإدارة التحريات والمباحث الجنائية بالقيادة العامة لشرطة الشارقة بأخذ إفادة المجني عليه بعد حصوله على عريضة من النيابة العامة بفتح البلاغ الجنائي عن الجرائم الإلكترونية، متى كان المجني عليه ضحية لها، وفي حال كان المتهم معلوماً يتم استدعاؤه لأخذ إفادته، فإذا كان الدليل الإلكتروني متوفراً تم تثبيته في محضر الاستدلالات، أما في حال حذف المحتوى أو الدليل الإلكتروني المجرم، فإنه يتم الرجوع إلى النسخ الاحتياطية للجهاز من خلال فحص الجهاز في المختبر لاستعادة النسخة الاحتياطية لحساب

20 مصطفى محمد موسى، دليل التحري عبر شبكة الإنترنت، دار الكتب القانونية، القاهرة، 2015م، ص 117.

21 محمد عبدالله إبراهيم، المواجهة الأمنية لجرائم شبكة المعلومات الدولية، أطروحة دكتوراه غير منشورة، كلية الدراسات العليا، أكاديمية الشرطة، القاهرة، 2016، ص 63.

22 موقع القيادة العامة لشرطة الشارقة https://www.shjpolice.gov.ae/. تاريخ زيارة الموقع: 2024/7/05.

المستخدم والمحتوى غير المشروع عن طريق الخبير التقني المختص. وفي حال التثبت من ارتكاب الجريمة الإلكتروني عبر جهاز لم يسلم لمأمور الضبط القضائي، فإنه يمكن تفتيش منزل المتهم بعد استصدار إذن من النيابة العامة، على أن يقوم القسم المختص بتحريز كافة الأجهزة محل ارتكاب الجريمة، أو التي تكون هناك قرائن قوية على ارتكاب الجريمة بواسطتها، تمهيداً لفحصها مختبرياً للتحصل على الأدلة الإلكتروني لإثبات الجريمة. أما في حال كان الجاني الذي قام بفعل السب أو القذف يستخدم اسمعاً مستعاراً، فيتم تتبع العنوان البروتوكولي لحساب المستخدم من خلال خطاب يوجه لهيئة تنظيم الاتصالات أو الجهة الأمنية المختصة في الدولة، فإذا ما تعذر الوصول إلى المتهم، يتم التواصل مع شركة الإنترنت التي ارتكبت الجريمة عبرها بطلب رسمي مشفوعاً بأسباب حاجة الجهة المختصة لبيانات المستخدم، والتي ترى من جهتها عدم وجوب إجابة طلب هذه الجهات، حيث أنها من الممكن أن ترفض تقديم المساعدة بإجابة الطلب بحجة أنها لا ترى في المحتوى انتهاكاً، هذا بالإضافة إلى دور فرع جرائم تقنية المعلومات بالقيادة العامة لشرطة الشارقة بالقيام بمهام الدوريات الإلكترونية والتي تجوب الشبكات ووسائل التواصل الاجتماعي وغيرها من المواقع الإلكترونية لرصد السلوكيات غير المشروعة، تمهيداً لاتخاذ الإجراءات القانونية في مواجهة مرتكبيها.

2). تجربة القيادة العامة لشرطة دبي:

تتمثل تجربة القيادة العامة لشرطة دبي في التعامل مع جرائم تقنية المعلومات، ومنها جرائم السب عبر الوسائل الإلكترونية، وذلك بعد تلقي البلاغ أو الشكوى الجنائية بأي طريقة كانت سواء قام المجني عليه بالذهاب إلى مركز الشرطة المختص أو بتقديم طلب فتح بلاغ/ شكوى جنائية في النيابة العامة من خلال طلب إلكتروني يقدم في صالة الخدمات الإلكترونية بمبنى النيابة العامة، أو عن طريق الموقع الإلكتروني لشرطة دبي www.dubaipolice.gov.ae أو عن طريق التطبيق الذكي لشرطة دبي Dubai Police للهواتف الذكية والأجهزة اللوحية.

وبعد قيام مأمور الضبط القضائي بفتح البلاغ الجنائي واتخاذ الإجراءات الإدارية اللازمة بالحصول على موافقة مدير المركز أو الضابط المختص بمخاطبة الجهات المعنية، تتم مراسلة المختبر الإلكتروني بالإدارة العامة للأدلة الجنائية وعلم الجريمة في شرطة دبي، حيث غالباً ما تكون المخاطبات إلكترونية طلباً بإثبات المحتوى محل البلاغ أو الشكوى، حيث يقوم مأمور الضبط القضائي المختص بالمراسلة بصياغة الطلب مرفقاً به حساب المستخدم المراد تفريغ محتواه المجرم بالإضافة إلى إرفاق الأدلة التي سبق وأن تقدم بها المبلغ عند طلبه فتح البلاغ أو الشكوى الجنائية، حيث يقوم الخبير التقني المختص بالدخول إلى الوسائل الإلكترونية أو نظام المعلومات الإلكتروني أو وسائل التواصل الاجتماعي التي تم ارتكاب جريمة السب أو القذف من خلالها، وذلك عن طريق حساب مستخدم يقوم الخبير باستخدامه لكي يتمكن من الإطلاع على المحتوى، وفي حال كان المحتوى لازال موجوداً، يقوم الخبير التقني المختص حينها بتفريغ الدليل بوسيلتين، هما:

- **الأولى:** عبر دعائم ورقية رسمية صادرة من المختبر بإمضاء الخبير ومسؤوله المباشر.
- **الثانية:** تفريغ ذات المحتوى عبر ملفات تحفظ في قرص مدمج CD مع إعداد تقرير تفصيلي عن النتيجة التي توصل إليها الخبير، ومن ثم إرسال التقرير والنتائج إلى مركز الشرطة المختص مرة أخرى.

أما عن المدة التي قد تستغرق في المراسلات الإدارية بين الجهات الإدارية المختصة، فإنها تطول أو تقصر بحسب سرعة الإنجاز لدى مركز الشرطة نفسه وضغط العمل لدى المختبر الإلكتروني، حيث أن هناك بلاغات وشكاوى جنائية إلكترونية لم تستغرق فيها المدة بين تلقي البلاغ إلى حيث ورود التقارير سوى أسبوعان على الأكثر، في حين أن هناك بلاغات أخرى امتدت المدة لما يقارب ستة أشهر، وربما في بعض البلاغات كانت المدة أطول من ذلك.

ويرى الباحث أنه بالرغم من طول الإجراءات في شرطة دبي، إلا أنه من الممكن إثبات الحالة طالما أن المحتوى المجرم كان لازال منشوراً عبر الوسائل الإلكترونية أو نظام المعلومات الإلكتروني أو وسيلة التواصل الاجتماعي، ويفضل عدم الانتظار لحين ورود تقرير المختبر الإلكتروني، حيث أن العديد من الأدلة الرقمية يتم حذفها خلال هذه المدة، في حين أنها كانت لازالت منشورة لحظة فتح البلاغ الجنائي، فإذا كان قيد البلاغ رسمياً لا يتم إلا بعد ورود تقرير المختبر الإلكتروني والذي قد يستغرق وقتاً طويلاً نسبياً في التعامل، حيث أن هذا النمط من الجرائم تتطلب السرعة في اتخاذ الإجراءات تجاه الجاني المبتز وعدم السماح له بالإفلات من أجهزة العدالة.

3). تجربة القيادة العامة لشرطة أبوظبي[23]

أما بالنسبة لفرع الجرائم الإلكترونية التابع لقسم الجريمة المنظمة بإدارة التحريات والمباحث الجنائية بشرطة أبوظبي، فهي لا تختلف عن مثيلاتها في الشارقة ودبي، حيث يتوجب على من يرغب بفتح بلاغ جنائي عن أي من جرائم تقنية المعلومات ومنها جرائم السب، الحصول على عريضة من النيابة العامة لفتح البلاغ/ أو الشكوى، ومن ثم يقوم الشاكي أو المبلغ بالتوجه إلى إدارة التحريات والمباحث الجنائية ليحصل على موافقة مدير الإدارة على فتح البلاغ، وبعد ذلك يتم أخذ إفادة المبلغ معززة بالدليل المتوفر لديه. ولا تثار أية إشكالية بالنسبة للمتهم المعلوم، إنما تثور ذات الإشكاليات السابق ذكرها بالنسبة للمتهم المجهول الذي يستخدم صفحات الإنترنت ومواقع التواصل الاجتماعي المتنوعة من خلال اسم مستعار أو بانتحال شخصية الغير، حيث يتم إتباع ذات الخطوات التي تتبعها كل من شرطة الشارقة وشرطة دبي في محاولة التوصل إلى شخص المتهم لاستدعائه.

ويرى الباحث أن تجربة شرطة دبي مثالية بشأن تفريغ المحتوى الإلكتروني – أو الدليل الرقمي – محل الاتهام في الجريمة الإلكترونية على مستخرج ورقي[24] رسمي صادر من المختبر الإلكتروني الجنائي التابع لشرطة دبي، الأمر

23 الموقع الرسمي للقيادة العامة لشرطة أبوظبي https://www.adpolice.gov.ae/. تاريخ زيارة الموقع: 2024/7/05.

24 تتمثل إجراءات استخراج الصور الرقمية وتقديمها كدليل لأجهزة العدالة الجنائية في 4 مراحل هي:

الذي يعزز من الدليل الرقمي، بالرغم من أنه يفترض عرض الدليل الإلكتروني على المحكمة أثناء نظر الموضوع ومجابهة المتهم به، إلا أنه نظراً لكون الدليل الإلكتروني في هذا النوع من الجرائم الإلكترونية قابل للحذف بلمح البصر، فقد ارتأت شرطة دبي إلى إثبات المحتوى محل الاتهام من خلال تفريغه على مستخرج رسمي يحمل شعار شرطة دبي، هذا بالإضافة إلى تخزين ذات المحتوى على دعامة إلكترونية يتم إرفاقها مع ملف الدعوى، وهذه الإجراءات متبعة في شرطة دبي سواء كان المتهم معروفاً أو مجهولاً، بينما تكمن الميزة في كل من القيادة العامة لشرطة أبوظبي والقيادة العامة لشرطة الشارقة، في سرعة اتخاذ الإجراءات مقارنة بإجراءات القيادة العامة لشرطة دبي، متى كان المتهم معروفاً، حيث يتم استدعاء المتهم بعد ورود البلاغ ببرهة يسيرة للإدلاء بإفادته ومتابعة إجراءات البحث والتحري الأخرى.

المطلب الثاني إجراءات المعاينة وضبط الأشياء والتفتيش في جرائم السب المعلوماتي

تختلف إجراءات المعاينة والتفتيش وضبط الأدلة الإلكترونية عن الجريمة التقليدية، حيث يتطلب من مأمور الضبط القضائي الإلمام والمعرفة بالحاسب الآلي والإنترنت وطبيعته وتشغيله، ومن هم الخبراء المناسبين الذي يندبهم. **وعليه سنوضح ذلك على النحو التالي:**

أولاً– الانتقال والمعاينة:

يقصد بالانتقال ذهاب المحقق إلى المكان الذي ارتكبت فيه الجريمة، حيث توجد آثارها وأدلتها، وتعني المعاينة مشاهدة وإثبات الحالة في مكان الجريمة، أي مشاهدة وإثبات الآثار المادية الذي خلفها ارتكاب الجريمة[25]، وتعتبر المعاينة دليلاً مباشراً ذات قيمة في إثبات الجريمة، حيث يتم عن طريقها مشاهدة وإثبات الحالة في موقع الجريمة، مما يفيد في الوصول إلى كشف الحقيقة وكل ما يتعلق بماديات الجريمة[26].

ولقد نصت المادة (43) من قانون الإجراءات الجزائية الإماراتي على الانتقال بقولها: (على مأمور الضبط القضائي في حالة التلبس بالجريمة أن ينتقل فوراً لمحل الواقعة ويعاين الآثار المادية للجريمة ويحافظ عليها ويثبت حالة الأماكن والأشخاص وكل ما يفيد في كشف الحقيقة ويسمع أقوال من كان حاضراً أو من يمكن الحصول منه على إيضاحات في شأن الواقعة ومرتكبيها، وعليه إخطار النيابة العامة فوراً بانتقاله، وعلى النيابة العامة الانتقال فوراً إلى محل الواقعة بمجرد إخطارها بجناية متلبس بها). كما نصت المادة (35) من ذات القانون على المعاينة بقولها:

1- مرحلة إعداد وتجهيز المعدات المستخدمة لاستخلاص الدليل الرقمي.

2- مرحلة ضبط واستخلاص الدليل الرقمي.

3- مرحلة حماية الدليل الرقمي من التلف أو العبث بمحتواه.

4- مرحلة تقديم الدليل الرقمي لأجهزة الشرطة والنيابة والقضاء.

ممدوح عبد الحميد، البحث والتحقيق في جرائم استخدام الكمبيوتر، دار الحقوق للنشر، الشارقة، 2001م، ص 18

25 لطيفة الجميلي، الوجيز في شرح قانون الإجراءات الجزائية الاتحادي، الآفاق المشرقة، الشارقة، 2013م، ص126.

26أسامة بن غانم العبيدي، التفتيش عن الدليل في الجرائم المعلوماتية، دراسة مقارنة، المجلة العربية للدراسات الأمنية والتدريب، جامعة نايف العربية للعلوم الأمنية، المجلد 29، العدد 58، يناير 2012م، ص 123.

(يجب على مأموري الضبط القضائي أن يقبلوا التبليغات والشكاوى التي ترد إليهم في شأن الجرائم، ويجب عليهم وعلى مرؤوسيهم أن يحصلوا على الإيضاحات وإجراءات المعاينة اللازمة لتسهيل تحقيق الوقائع التي تبلغ إليهم أو التي يعملون بها بأية كيفية كانت، وعليهم أن يتخذوا جميع الوسائل التحفظية اللازمة للمحافظة على أدلة الجريمة). ونصت المادة (44) من ذات القانون على أمر المنع من مبارحة محل وقوع الجريمة بقولها: (لمأمور الضبط القضائي عند انتقاله في جريمة متلبس بها أن يمنع الحاضرين من مبارحة محل الواقعة أو الابتعاد عنه حتى يتم تحرير المحضر وله أن يستدعي في الحال من يمكن الحصول منه على إيضاحات في شأن الواقعة، فإذا خالف أحد الحاضرين الأمر الصادر إليه من مأمور الضبط القضائي أو امتنع أحد ممن دعوا عن الحضور، يثبت ذلك في المحضر ويعرض الأمر على النيابة العامة لاتخاذ ما تراه. وتحكم المحكمة المختصة على المخالف أو الممتنع بعد تحقيق دفاعه بغرامة لا يجاوز مقدارها خمسمائة درهم).

وعليه يستنتج الباحث أن التعامل مع مسرح الجرائم الإلكترونية ومعاينته تختلف في بعض الإجراءات عن مسرح الجريمة التقليدية، حيث التعامل مع البرامج والبيانات الرقمية يحتم الانتقال إلى العالم الافتراضي أو الإلكتروني للحصول على المعلومات وجمع الاستدلالات، وهذا يتطلب من المحقق أو مأمور الضبط القضائي نوع من الإلمام والمعرفة بالعالم الفضاء الإلكتروني.

ويرى جانب من الفقه ضرورة إتباع بعض القواعد والإرشادات الفنية عند معاينة مسرح الجريمة الإلكترونية، وتتمثل هذه الإجراءات في الآتي:[27]

- القيام بفحص الحاسب الآلي وما قد يتصل به من أجهزة طرفيه ومحتوياته وأوضاع المكان الذي يوجد به بصفة عامة مع العناية بتصوير أجزائه الخلفية وملحقاته الأخرى، على أن يراعى تسجيل الزمان والتاريخ والمكان الذي تم التقاط الصور فيه.
- ملاحظة طريقة إعداد نظام الحاسب الآلي بعناية بالغة.
- إثبات الحالة التي تكون عليها توصيلات الحاسب الآلي، والتي تكون متصلة بمكونات النظام المعلوماتي، وذلك حتى يسهل القيام بعملية مقارنة وتحليل لبياناتها عند عرض الموضوع على النيابة أو المحكمة المختصة.
- عدم التسرع في نقل أي مادة معلوماتية من مكان وقوع الجريمة، وذلك قبل إجراء الاختبارات اللازمة للتيقن من عدم وجود أي مجالات مغناطيسية في المحيط الخارجي، حتى لا يحدث أي إتلاف للبيانات المخزنة.

27 أسامة بن غانم العبيدي، التفتيش عن الدليل في الجرائم المعلوماتية، مرجع سابق، ص 145.

- حفظ ما تحويه سلة المهملات من الأوراق الملقاة أو الممزقة وأوراق الكربون المستعملة والشرائط والأقراص الممغنطة غير السليمة أو المحطمة وفحصها، ورفع البصمات التي قد تكون لها علاقة بالجريمة المرتكبة، لأن دليل الجهة قد يكمن في مكافحة هذه القصاصات.
- القيام بحفظ المستندات الخاصة بالإدخال وكذلك مخرجات الحاسب الآلي الورقية التي قد تكون ذات صلة بالجريمة، من أجل رفع ومضاهاة البصمات التي قد تكون موجودة عليها.
- يجب قصر عملية المعاينة على مأموري الضبط القضائي، سواء كانوا من الباحثين أو المحققين ممن تتوفر فيهم الكفاءة العلمية والخبرة الفنية في مجال الحاسبات واسترجاع المعلومات، ممن تلقوا التدريب الكافي في مجال الحاسبات واسترجاع المعلومات ومواجهة هذه النوعية من الجرائم والتعامل مع أدلتها التي قد تتخلف عنها على مسرح الجريمة.

ومن المهم هنا أن يتم توثيق مسرح الجريمة الإلكترونية، ووصفه بكامل محتوياته بشكل جيد، مع توثيق كل دليل على حدة بما فيها الأدلة الرقمية، بحيث يتم توضيح مكان الضبط والهيئة التي كان عليها، ومن قان برفعه وتحريزه وكيف ومتى تم ذلك، بل إن البعض[28] يرى أن التوثيق يجب أن يشمل كافة المصادر المتاحة على الشبكة التي ترتبط بها الأجهزة محل التحقيق.

ثانياً– التفتيش وضبط الأدلة الإلكترونية:

يعتبر التفتيش أخطر الإجراءات الماسة بالحرية الشخصية، لكونه يمثل قيداً وجوبياً يخضع له الشخص، لذلك يعد التفتيش من مسؤوليات السلطة القضائية، ولا يجوز القيام به إلا بأمر قضائي صادر من السلطة القضائية المختصة أو بناءً على نص قانوني صريح، ولا يصدر أمر التفتيش القضائي للأماكن والأشخاص، إلا بعد تسجيل بلاغ بوقوع جريمة معينة، وبعد تحريك الدعوى الجنائية، ويصدر أمر التفتيش موضحاً الجهة التي تتولى تنفيذ إجراءات التفتيش محدد المكان الذي يجري تفتيشه ومسمياً الأشخاص أو الأشياء التي يجرى البحث عنها[29].

ونظراً لكون التفتيش يعد إجراءً من إجراءات التحقيق الابتدائي، فإنه لا يجوز تقريره إلا للبحث عن الأشياء الخاصة بالجريمة الجاري جمع الاستدلالات أو التحقيق بشأنها، فلا يجوز إجراء التفتيش للتوصل إلى ضبط جريمة مستقبلية أو للوقاية من وقوعها، ومع ذلك إذا ظهر عرضاً أثناء التفتيش وجود أشياء تعد حيازتها جريمة، أو تفيد في كشف الحقيقة في جريمة أخرى، قام مأمور الضبط القضائي بضبطها[30].

ولقد تطلب المشرع الإماراتي في المادة (73) من قانون الإجراءات الجزائية الاتحادي، لصحة التفتيش حضور المتهم أو من ينيب عنه، وإذا تعذر حضوره جرى التفتيش بحضور شهود كلما أمكن ذلك، ويكون هؤلاء الشهود

28 عبدالله حسين علي، سرقة المعلومات المخزنة في الحاسب الآلي، دار النهضة العربية، القاهرة، 2012، ص 256.

29 أسامة بن غانم العبيدي، التفتيش عن الدليل في الجرائم المعلوماتية، مرجع سابق، ص 139

30 ممدوح السبكي، حدود سلطات مأمور الضبط القضائي في التحقيق، دار النهضة العربية، القاهرة، 1998، ص 76

بقدر الإمكان أقاربه البالغين أو من أحد سكان العقار الذي يقطنه أو من الجيران ويتم إثبات ذلك في المحضر. حيث نصت تلك المادة على أن: "يحصل تفتيش منزل المتهم بحضوره أو حضور من ينوب عنه كلما أمكن ذلك وإذا حصل تفتيش في منزل غير منزل المتهم يدعي صاحبه إلى الحضور بنفسه أو بواسطة من ينيبه كلما أمكن ذلك".

ويخضع مأمورو الضبط القضائي في مباشرتهم لوظيفة الضبطية القضائية المتعلقة بإجراءات جمع الاستدلالات لإشراف النيابة العامة، وهو ما أكدته المادة (94) والمادة (20) على إعطاء الحق للسلطة القضائية بتفتيش المتهم، فالمشرع الإماراتي أعطى هذا الحق للنيابة العامة على اعتبارها هي جهة التحقيق الوحيدة، وقد نصت على ذلك المادة (5) من قانون الإجراءات الجزائية الإماراتي بقولها: "النيابة العامة جزء من السلطة القضائية وتباشر التحقيق والاتهام في الجرائم وفقاً لأحكام هذا القانون".

ويلاحظ أن تبعية مأموري الضبط للنيابة العامة ليست تبعية إدارية وإنما وظيفية، فالتبعية الإدارية تكون لرؤسائهم الإداريين بوزارة الداخلية، أما النيابة العامة فهي تختص فقط بالإشراف على وظيفة الضبطية القضائية من حيث الاستدلال والندب للتحقيق، وهذه التبعية والخضوع لإشراف النيابة العامة تعلل بكون مأموري الضبط القضائي يباشرون عملهم من أجل تمكين النيابة بوصفها سلطة التحقيق من مباشرة عملها واتخاذ قرارها في شأن تحريك الدعوى الجنائية، أي أن غاية عملهم هي إمداد النيابة العامة بعناصر التقدير، ومن ثم فإن نشاطها لحساب النيابة العامة، كما تعلل أيضًا بكون الثقافة القانونية لأعضاء النيابة العامة وخبرتهم تجعلهم أحرص وأدق من مأموري الضبط القضائي على التطبيق الصحيح للقانون واحترام الحقوق والحريات الفردية[31].

ولقد راعت أغلب التشريعات الجزائية ومنها التشريع الإماراتي – أثناء إجراء التفتيش – ضرورة الموازنة بين ضمانة حماية حريات الأشخاص وحرمة مساكتهم، وبين المصلحة العامة للمجتمع في الكشف عن الجريمة للوصول إلى الحقيقة[32].

وعليه يرى الباحث في هذا الشأن ضرورة مراعاة القواعد والشروط الموضوعية والشكلية عند إجراء التفتيش في الجرائم الإلكترونية، ومنها جريمتي السب، وذلك حتى تتحقق الموازنة التي يحرص عليها المشرع الجزائي، إذ أن مخالفة هذه الشروط والقواعد يترتب عليها بطلان إجراءات التفتيش وما ينتج عنها من آثار.

وفي إطار جرائم تقنية المعلومات ومنها جريمتي السب، فإن التفتيش يقع على القطع الصلبة وهو جهاز الحاسب الآلي والأجهزة المتصلة به والشبكة والبرامج أو المكونات المنطقية للحاسب الآلي من بيانات ومعلومات، **وسنوضح ذلك كالتالي:**

---

31 لطيفة الجميلي، الوجيز في شرح قانون الإجراءات الجزائية الاتحادي، مرجع سابق، ص 131

32 المواد (221-223-225) من قانون الإجراءات الجزائية الإماراتي.

1- تفتيش المكونات المادية للحاسب الآلي:

يقصد بالمكونات المادية للحاسب الآلي تلك الأجزاء المادية الملموسة للجهاز، وتقسم إلى عدة أجزاء، هي: (1- وحدة المعالجة المركزية التي يوكل إليها التحكم بالعمليات التي تتم داخل الجهاز ومسئولة عن القيام بمعالجة المعلومات بعد استقبالها من وحدات الإدخال ثم إرسالها إلى وحدات التخزين والإخراج، 2- وحدات الإدخال والتي تتكون من لوحة المفاتيح والفأرة والماسح الضوئي، 3- وحدات الإخراج والتي يتم إخراج المعلومات منها على شكل يفهمه الإنسان ومنها الشاشة والطابعة، 4- وحدات التخزين الثانوية كالأقراص الصلبة والمدمجة، 5- وسائط الاتصال وتتمثل في الكابلات والأسلاك التي تربط بين الأجزاء المختلفة لجهاز الحاسب الآلي)[33].

وليس هناك خلاف على أن الدخول إلى المكونات المادية للحاسب الآلي بحثاً عن شيء ما يتصل بجريمة سب أو قذف وقعت يفيد في كشف الحقيقة عنها وعن مرتكبها ويخضع للإجراءات القانونية الخاصة بالتفتيش، بمعنى أن حكم تفتيش تلك المكونات المادية للحاسب الآلي يتوقف على طبيعة المكان الموجودة فيه تلك المكونات المادية، وهل هو من الأماكن العامة أو من الأماكن الخاصة، حيث أن وصف المكان وطبيعته أهمية قصوى خاصة في مجال التفتيش عن الجرائم الإلكترونية، فإذا كانت موجود في مكان خاص كمسكن المتهم أو أحد ملحقاته كان لها حكمة، فلا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش مسكنه، وبنفس الضمانات والإجراءات المقررة قانوناً في التشريعات المختلفة، ما المكونات المادية للحاسب الآلي المحمول والهاتف المتحرك وكاميرات الفيديو أو التصوير، فهي تخضع لقواعد تفتيش الأشخاص[34].

وهنا يجب التفرقة بين ما إذا كان شخص المتهم أو شخص آخر غير المتهم، حيث يجب مراعاة القواعد الخاصة بكل حالة على حدة، كما يجب التفرقة بين ما إذا كانت هذه المكونات المادية لهذه الأجهزة متصلة بنهاية طرفية موجودة مع شخص آخر، حيث تخضع لقواعد تفتيش شخص غير المتهم بالنسبة لهذه النهاية الطرفية وبين ما إذا كانت متصلة بنهاية طرفية موجودة في مكان آخر، حيث تخضع لقواعد تفتيش الأماكن بالنسبة لهذه النهاية الطرفية[35].

وقد أشارت المادة (65) من المرسوم بقانون اتحادي رقم (34) لسنة 2021 بشأن مكافحة الشائعات والجرائم الإلكترونية إلى أن للأدلة المستخرجة من الأجهزة والوسائط الإلكترونية والأنظمة المعلوماتية والشبكات والبرامج الإلكترونية حجية الأدلة الجنائية المادية في الإثبات الجنائي، حيث نصت على أنه: "يكون للأدلة المستمدة أو المستخرجة من الأجهزة أو المعدات أو الوسائط أو الدعامات الإلكترونية أو النظام المعلوماتي أو برامج الحاسب الآلي أو من أي وسيلة لتقنية المعلومات حجية الأدلة الجنائية المادية في الإثبات الجنائي).

---

33 مكـونات الحاسـب الآلي"، الموسـوعة العربية الشـاملة، مقـال منشـور على الموقع الإلكتروني: www.mosoah.com/computer-and-electronics/computer-hardware - تاريخ زيارة الموقع: 2024/7/05.

34 هلالي عبد اللاه أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية، مرجع سابق، ص 91.

35 ممدوح عبد الحميد، البحث والتحقيق في جرائم استخدام الكمبيوتر وشبكة المعلومات العالمية، مرجع سابق، ص 69.

2- تفتيش المكونات غير المادية للحاسب الآلي:

يقصد بالمكونات غير المادية للحاسب الآلي تلك البرمجيات التي تقوم بعملية التحكم في عمليات الحاسب الآلي، وتتكون من عدة أجزاء رئيسية هي: (1- أنظمة التشغيل وهي تلك البرمجيات التي تكون في العادة مخزنة في ذاكرة القراءة فقط، وتقوم بعملية إدارة وتوجيه أجزاء الحاسب الآلي للقيام بكافة وظائفه على الشكل الصحيح. 2- الأنظمة التطبيقية كبرنامج معالجة النصوص Word وبرنامج Excel على سبيل المثال، وكذلك لغات البرمجة المختلفة)[36].

والجدير بالذكر أن النتيجة التي تنتهي إليها إجراءات التفتيش في جرائم تقنية المعلومات هي ضبط وتحريز الأدلة المعلوماتية التي تم الحصول عليها حال الوصول إليها، وفي هذه الحالة يلزم اتخاذ إجراءات معلوماتية محددة لكي يمكن القيام بضبط الأدلة المعلوماتية، فلا تصلح الإجراءات المادية المعرفة للقيام بضبط الأدلة كما هو الشأن في العالم المادي، باستثناء عملية الفصل الضرورية واللازمة بين الحاسب وبين كل شخص ليس له علاقة بالقائمين على الدعوى الجزائية، وذلك خشية قيام المتهم أو من له علاقة أو مصلحة ما بتدمير الأدلة وإزالتها من الحاسب الآلي[37].

ولقد نصت المادة (61) من قانون الإجراءات الجزائية الإماراتي على أن: (لمأموري الضبط القضائي أن يضبطوا الأشياء التي يحتمل أن تكون قد استعملت في ارتكاب الجريمة أو نتجت عن ارتكابها أو يحتمل أن تكون قد وقعت عليها الجريمة وكذلك كل ما يفيد في كشف الحقيقة)، ووفق هذا النص فإن هدف التفتيش هو ضبط الأشياء التي تفيد في كشف الحقيقة، أو الأشياء التي تعد في ذاتها دليلاً على الجريمة أو يمكن استخراج هذا الدليل منها[38].

وبناءً عليه، يرى الباحث أنه يجب أن تخضع كافة الأشياء ذات الصلة بالحاسب الآلي كـ(وحدة المدخلات – الملفات الإلكترونية – العمليات الإلكترونية – الذاكرة – وحدة التحكم – المودم – الشرائط الممغنطة – الطابعات – البرامج والتطبيقات – المراسلات الإلكترونية وغيرها) لإجراءات ضبط الأشياء في جرائم تقنية المعلومات، والتي تعد كيانات ذات قيمة يمكن الاستفادة منها في إثبات جريمة السب أو القذف الإلكتروني ونسبتها إلى الجاني.

---

36 مكـونات الحاسـب الآلي"، الموسـوعة العربية الشـاملة، مقـال منشـور على الموقع الإلكتروني: www.mosoah.com/computer-and-electronics/computer-hardware - تاريخ زيارة الموقع: 2024/7/05.

37 جلال الزعبي، أسامة المناعسة، جرائم تقنية نظم المعلومات الإلكترونية، مرجع سابق، ص 191

38 تختلف وسائل كشف وجمع الأدلة وإثبات الجرائم التي تعتمد على الحاسب الآلي أياً كان دوره في الجريمة على عديد من الوسائل الحديثة، فمنها ملفات الالتصاق الإلكتروني الخاصة بالتتبع على شبكات الإنترنت، ومنها الأشكال المختلفة للدليل الإلكتروني سواء كان مادياً في شكل قرص صلب أو محتوى معنوي، أو ملفات التسجيل والتصنت على البريد الإلكتروني كتقنية برنامج "كارينفور" التي تستخدمها الجهات الأمنية في كل من أمريكا وبريطانيا، وكذلك برامج معالجة الملفات وبرامج النسخ والاستعادة.

المبحث الثاني :التعاون الدولي بين أجهزة الشرطة لمواجهة جريمتي السب المعلوماتي

إن التعاون الدولي هو السبيل الفعال لمكافحة الجرائم المعلوماتية، ولذلك أبرمت العديد من الاتفاقيات الدولية في مجال التعاون الدولي، تستهدف التقريب بين القوانين الجنائية الوطنية من أجل مكافحة الجرائم عابرة الحدود، وتظهر معالم هذا التقارب في قبول حالات تفويض الاختصاص في اتخاذ إجراءات التحقيق وجمع الأدلة وتسليم المجرمين والاعتراف بالأحكام الجنائية الأجنبية، وهذا التعاون الدولي لا ينال من سيادة الدولة، بل على العكس فإن انعدام هذا التعاون يزيد من التباعد بين الأنظمة العقابية، مما يساعد على تزايد الجرائم عابرة الحدود ومنها جرائم المعلوماتية[39].

وفي هذا الإطار، **تلتزم وزارة الداخلية بدولة الإمارات العربية المتحدة** بالحفاظ على سرية وخصوصية جميع البيانات والمعلومات التي يتم تداولها بين قطاعاتها الأمنية المختلفة من خلال مختلف المواقع والأنظمة الإلكترونية وصفحات الويب المملوكة للوزارة، وتطبق الوزارة أعلى المعايير العالمية في إدارة أمن وحماية البيانات من خلال اعتمادها على أفضل تطبيقات وبرامج الأمن والحماية، وذلك لتوفير بيئة عمل آمنة تكفل قدراً عالياً من السرية والخصوصية، وتطبق الوزارة الداخلية أقصى التدابير الوقائية والاحترازية التي تمنع تعرض البيانات للخطر من خلال أنظمة حديثة، كما تواكب أي متغيرات تطرأ على بيئة العمل من خلال تعديل سياسات أمن البيانات بين الحين والآخر، للتحقق من شموليتها وعدم احتوائها على أية ثغرات فنية أو قانونية[40].

وسنتناول فيما يلي أهم مظاهر التعاون الدولي بين أجهزة الشرطة في مجال مواجهة جريمتي السب المعلوماتي، وذلك من خلال الآتي:

المطلب الأول: التعاون الأمني على المستوى الدولي في مجال مكافحة الجرائم المعلوماتية

يصعب على الأجهزة الشرطية في أي دولة القضاء على جرائم المعلوماتية عابرة الحدود بمعزل عن الأجهزة الشرطية في الدول المختلفة، لأن جهاز الشرطة يصعب عليه تعقب المجرمين ومتابعتهم إذا ما عبروا حدود الدولة، ولذلك فإن الحاجة ملحة إلى تعاون أجهزة الشرطة بين الدول وتنسيق العمل فيما بينها لضبط المجرمين، ومكافحة نشاط الإجرام المعلوماتي الذي يتجاوز حدود الدولة، لذلك أصبحت الحاجة ماسة إلى وجود كيان دولي يأخذ على عاتقه القيام بهذه المهمة وتتعاون من خلاله أجهزة الشرطة في الدول المختلفة، خاصة فيما يتعلق بتبادل المعلومات المتعلقة بالجريمة والمجرمين بأقصى سرعة ممكنة، بالإضافة إلى تعقب المجرمين الفارين من وجه العدالة، وقد تبلور هذا النوع من التعاون الدولي في إنشاء المنظمة الدولية للشرطة الجنائية (الإنتربول Interpol) والجهاز الأوروبي

---

39 هلالي عبد اللاه أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية، مرجع سابق، ص 186.

40 سياسة الخصوصية في وزارة الداخلية بدولة الإمارات: https://www.moi.gov.ae/SD/ar/home/PrivacyPolicy تاريخ زيارة الموقع: 2024/7/05.

للتعاون الشرطي في مواجهة جرائم الإنترنت (الأورجست Eurojust)، وعلى المستوى العربي يوجد مجلس وزراء الداخلية العرب (AIMC) لمكافحة جرائم تقنية المعلومات[41].

وفيما يلي نوضح دور وجهود هذه الأجهزة في مكافحة الجرائم الإلكترونية:

1. المنظمة الدولية للشرطة الجنائية (الإنتربول Interpol): تعتبر هذه المنظمة من أهم أجهزة التعاون الشرطي المكلفة بمكافحة الإجرام بصفة عام والجرائم الإلكترونية بصفة خاصة، وتهدف هذه المنظمة إلى تأكيد وتشجيع التعاون المتبادل بين سلطات الأمن في الدول الأطراف على نحو فعال يحقق مكافحة الجريمة، وإقامة وتنمية النظم التي من شأنها أن تسهم على نحو فعال في منع ومكافحة جرائم القانون العام، وهي تباشر ذلك أو تحقق ذك من خلال وظيفتين هما: القيام بتجميع كافة البيانات والمعلومات المتعلقة بالجريمة من خلال المكاتب المركزية الوطنية للشرطة الجنائية الدولية المتواجدة في أقاليم الدول الأعضاء، والتعاون في ضبط وملاحقة المجرمين الهاربين وتسليمهم إلى الدولة التي تطلب تسليمهم[42].
2. الجهاز الأوروبي للتعاون الشرطي (الأورجست Eurojust): يتواجد على المستوى الأوروبي (الأورجست Eurojust) الذي تم إنشاءه في عام 2002 من قبل المجلس الأوروبي كجهاز يساعد على التعاون القضائي والشرطي في مكافحة جميع أنواع الجرائم الإلكترونية، وتنعقد اختصاصاته عندما يمس ذلك الإجرام دولتين على الأقل من الدول الأعضاء في الاتحاد الأوروبي أو دولة عضو مع دولة من دول العالم الثالث أو دولة عضو مع الرابطة الأوروبية، وهي في ذلك غير مقتصرة على الأشخاص فقط، وإنما تشمل كذلك المؤسسات، لاسيما المؤسسات المالية والاقتصادية التي تتعرض لعمليات الاحتيال والسرقة الإلكترونية، ويمثل (الأورجست Eurojust) دعامة في فعالية التحقيقات والمطاردات المتبعة من قبل السلطات القضائية الوطنية في دول الاتحاد الأوربي، وخصوصاً فيما يتعلق بالأنشطة المتعلقة بجرائم الإنترنت، وهو في ذلك على علاقة وثيقة مع مركز الشرطة الأوروبية (EUOPL) الذي يمده بالتحليلات والبيانات والمعلومات اللازمة للقيام بالتحقيقات في تلك الجرائم[43].
3. مجلس وزراء الداخلية العرب (AIMC): تأسس مجلس وزراء الداخلية العرب خلال المؤتمر الثالث الذي عقد بالطائف في السعودية عام 1980م، ويعد مجلس الوزراء الداخلية العرب الهيئة العليا للعمل العربي المشترك في مجال مكافحة الجريمة وتحقيق الأمن الداخلي والأمن الإقليمي فيما بين الدول العربية، وهو من أهم المنظمات الأمنية التابعة لجامعة الدول العربية ويختص المجلس بإقرار التوصيات والمقترحات الصادرة من مختلف الهيئات العامة في المجالات الأمنية، وفي عام 2010 عقد مجلس الوزراء الداخلية

41 محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، مرجع سابق، ص 226

42 حسين سعيد الغافري، السياسة الجنائية في مواجهة جرائم الإنترنت، مرجع سابق، ص 118.

43 حوراء موسى، الجرائم المرتكبة عبر وسائل التواصل الاجتماعي، مرجع سابق، ص 339.

العرب اجتماعاً في مدينة القاهرة للتباحث في أوضاع الجريمة في الدول العربية ومناقشة الاتفاقيات المطروحة وأسفر الاجتماع عن التوقيع على (5) اتفاقيات من بينها الاتفاقية العربية لمكافحة جرائم تقنية المعلومات[44]، وتشمل هذه الاتفاقية على (43) مادة، وتهدف هذا الاتفاقية إلى تعزيز أواصر التعاون وتدعيمه بين الدول العربية في مجال مكافحة الجرائم تقنية المعلومات، لدرء خطر هذه الجرائم حفاظاً على أمن الدول العربية ومصالحها وسلامة مجتمعها وأفرادها[45]، وحول تبادل المعلومات بين الدول العربية لمكافحة جرائم تقنية المعلومات نصت المادة (1.2.3/32) على ما يلي: تلتزم كل دولة عربية طرف بتبني الإجراءات الضرورية من أجل تطبيق الالتزامات الواردة في الاتفاقية، وعلى جميع الدول الأطراف تبادل المساعدة فيما بينها بأقصى مدي ممكن من لغات التحقيقات أو الإجراءات المتعلقة بجرائم معلومات وتقنية المعلومات أو لجمع الأدلة الإلكترونية في الجرائم، ويتم تقديم طلب المساعدة الثنائية والاتصالات المتعلقة بها بشكل خطي، ويجوز لكل دولة طرف في تلك الحالة الطارئة أن تقدم هذا الطلب بشكل عاجل، على أن تضمن هذه الاتصالات القدرة المعقولة من الأمن والمرجعية (بما في ذلك استخدام التشفير) وتأكيد الإرسال حسبما تطلب الدول الطرف، ويجب على الدولة الطرف المطلوب منها المساعدة أن تقبل وتستجيب للطلب بوسيلة عاجلة من الاتصالات، كما نصت المادة (1/43) من الاتفاقية على إلزام الدول العربية بإنشاء جهاز متخصص ومتفرع على مدار الساعة في كل دولة لضمان توفير المساعدة الفورية لغاية التحقيق أو الإجراءات المتعلقة بجرائم تقنية المعلومات أو لجمع الأدلة بشكلها الالكتروني في جريمة معينة». وحول تسليم المجرمين بين الدول العربية نصت المادة (31) على ما يلي: 1- هذه المادة تنطبق على التبادل المجرمين بين الدول الأطراف على الجرائم المنصوص عليها في هذه الاتفاقية بشرط أن تكون تلك الجرائم يعاقب عليها في القانون الدول الأطراف المعنية بسلب الحرية لفترة أدناها سنة واحدة أو عقوبة أشد. وإذا انطبقت عقوبة أدنى مختلفة حسب ترتيب متفق عليه أو حسب معاهدة تسليم المجرمين فإن العقوبة الدنيا هي التي سوف تطبق. 2- إن الجرائم المنصوص عليها في الفقرة (1) من هذه المادة تعتبر جرائم قابلة لتسليم المجرمين الذين يرتكبونها ف أية معاهدة لتسليم المجرمين قائمة بين الدول الأطراف. 3- إذا قامت دولة طرف كما يجعل تسليم المجرمين مشروطاً بوجود معاهدة تسليم فيمك ن اعتباره هذه الاتفاقية كأساس قانوني لتسليم المجرمين فيما يتعلق بالجرائم المذكورة في الفقرة (1) من هذه المادة. 4- الدول الأطراف التي لا تشترط وجود معاهدة لتبادل المجرمين يجب أن تعتبر الجرائم المذكورة في الفقرة (1) من هذه الشروط المنصوص عليها في قانون الدولة الطرف التي يقدم إليها الطلب أو المعاهدات التسليم المطبقة بما في ذلك الأسس التي يمكن للدولة الطرف الإسناد عليها لرفض تسليم المجرمين[46]. كما نصت المادة (1/43) من الاتفاقية على إلزام الدول العربية بإنشاء جهاز

44 عبد الكريم خالد الردايدة، الجرائم المستحدثة وإستراتيجية مواجهتها، دار الحامد للنشر، عمان، 2015م، ص 114.

45 المادة (1) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010.

46 المادة (31) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010

متخصص ومتفرغ على مدار الساعة في كل دولة لضمان توفير المساعدة الفورية لغاية التحقيق أو الإجراءات المتعلقة بجرائم تقنية المعلومات أو لجمع الأدلة بشكلها الالكتروني في جريمة معينة، ويجب أن تشمل مثل هذه المساعدة تسهيل أو تنفيذ ما يلي: (توفير المشورة الفنية، حفظ المعلومات، جمع الأدلة وإعطاء المعلومات القانونية وتحديد مكان المشبوهين)، وحول العقوبات التي توقع على مرتكبي الجرائم تقنية المعلومات ألزمت الاتفاقية الدول العربية بترتيب المسؤولية الجزائية للأشخاص الاعتبارية عن الجرائم التي يرتكبها ممثلوها باسمها أو لصالحها دون الإخلال بفرض العقوبة على الشخص الطبيعي الذي يرتكب الجريمة شخصيا. كما ألزمت الاتفاقية بتشديد العقوبات على الجرائم التقليدية في حال ارتكابها بإحدى الوسائل الإلكترونية أو وسائل تقنية المعلومات.

وعلى الرغم من تعدد الأجهزة الأمنية الدولية في مكافحة الجرائم الإلكترونية، إلا أن البعض يرى أن هناك صعوبة في التعاون الدولي في مكافحة تلك الجرائم، وذلك للأسباب الآتية[47]:

1. عدم وجود تعاون فيما بين الدول بخصوص الإجراءات الجنائية بين الدول المختلفة، لاسيما بالنسبة لأعمال الاستدلال والتحقيق، وضرورة الحصول على موافقة خارج حدود الدولة حتى يتسنى للمحقق التفتيش في نظام معلوماتي لدولة أخرى.
2. قصور الدول في عقد المعاهدات الثنائية والجماعية إلى الحد الذي يسمح بالتعاون فيما بينهم، وحتى في حالة وجود هذه المعاهدات، فإنها لا تكون كافية بالقدر اللازم لمواجهة التقدم الكبير في الجرائم الإلكترونية، ومن ثم لا تؤتي هذه المعاهدات آثارها الإيجابية.
3. غياب مفهوم واضح ومحدد للجريمة الإلكترونية، فكافة التشريعات الوطنية لم تتفق على مفهوم واضح ومحدد لمفهوم "إساءة استخدام نظم المعلومات"، وتختلف الدول فيما بينها حول النشاط الذي ينبغي تجريمه في دولة ما عن الأخرى وفقاً للعادات والتقاليد الدولية.
4. مشكلة الاختصاص في جرائم الإلكترونية وهي من المشكلات التي تعرقل الحصول على الدليل المعلوماتي، وهذه المشكلة تعد من أهم الصعوبات التي تواجه رجال البحث الجنائي في مجال الجريمة الإلكترونية، وخاصة في حالة الاعتداء على البيانات المخزنة داخل أجهزة الحاسب الآلي وما تمثله من اعتداء على حرمة الحياة الخاصة.

ويرى الباحث أن التعاون الأمني على المستوى العربي في مكافحة الجرائم الإلكترونية مطلب أساسي وضروري، حيث أن الأمن الداخلي والخارجي لكل دولة عربية مرتبط بالأمن العربي الجماعي، وأن الإخلال بالأمن الداخلي في أي دولة تتعدى آثاره بالضرورة إلى الإخلال بالاستقرار في كافة نواحي الحياة، مما يؤثر في النهاية على محصلة

47 حسين سعيد الغافري، السياسة الجنائية في مواجهة جرائم الإنترنت، مرجع سابق، ص 178.

القوة الذاتية للدول العربية كافة، وعليه يجب أن تلتزم كل دولة عربية بتبني الإجراءات الضرورية من أجل تطبيق الالتزامات الواردة في الاتفاقية، وتقديم المساعدة والاتصالات الأمنية اللازمة لمكافحة جرائم تقنية المعلومات».

أما عن جهود وزارة الداخلية بدولة الإمارات العربية المتحدة في مكافحة جرائم تقنية المعلومات، نجد أنه في عام 2002م أنشئت الوزارة أقسام للجريمة المنظمة وأفرع للجرائم الإلكترونية بالقيادات والإدارات الأمنية في الدولة، حيث أخذت تلك الأقسام المتخصصة في مكافحة الجرائم الإلكترونية على انتهاج سياسة التقدم ومواكبة التطور العلمي والتكنولوجي من خلال الاعتماد على التقنيات الحديثة ولمواجهة كافة الصور المستحدثة من الجرائم عبر الحاسب الآلي والإنترنت وخاصة المتعلقة بفئة الأطفال والشباب، كما كرست وزارة الداخلية جهودها حتى أصبحت عضواً في (القوة العالمية الافتراضية VGT في مارس 2010م) والتي تمثل شراكة دولية من وكالات إنفاذ القانون والمنظمات غير الحكومية والجمعيات الأهلية، للمساعدة في حماية أفراد المجتمع من الاعتداءات غير المشروعة التي قد يتعرضون لها عبر شبكة الإنترنت وغيرها من أشكال الاستغلال والتهديد الإلكتروني العابر للحدود، كما استضافت دولة الإمارات مؤتمر (VGT) في عام 2012، وسعت للقيام بكل ما في وسعها لبناء القدرات والإمكانيات في هذا المجال، وشجعت الشركاء على بذل المزيد من الجهود في هذا الجانب، وهدفت وزارة الداخلية من الانضمام إلى هذا التحالف العالمي لمكافحة الاعتداءات غير المشروعة عبر وسائل تقنية المعلومات وشبكة الإنترنت إلى تعزيز جهودها للتحقيق في حالات الاعتداء غير المشروع عبر الإنترنت، وتحديد وملاحقة الجناة وتحديد هوية الضحايا وضمان حصولهم على ما يلزم من المساعدة والدعم والحماية[48].

وإلى جانب ذلك، عملت وزارة الداخلية عن كثب مع هيئة تنظيم الاتصالات في الدولة لمراقبة وحجب المواقع المنافية للآداب، وبذل الجهود لرصد أي استغلال غير مشروع عبر شبكة الإنترنت، وأي محاولات للاعتداء عليهم من قبل مرتكبي الجرائم ممن ينطبق عليهم القانون الاتحادي رقم (34) لسنة 2021 بشأن مكافحة الشائعات والجرائم الإلكترونية، كما سعت إلى نشر الوعي عن الاستخدام الأمثل للإنترنت بين الأسر والأفراد، وهناك العديد من الجهود الرامية إلى السيطرة على هذا النوع من الجرائم بالشراكة مع الجهات المختلفة، فضلاً عن إطلاق العديد من المبادرات التي تساعد على زيادة حماية الأطفال والأطفال من إساءة استخدام الإنترنت، وجعل حياتهم أفضل[49].

وتبرز جهود وزارة الداخلية في هذا الصدد، في إطار الدور الرقابي لجهود الدولة في تحقيق التوجهات المستقبلية لحكومة الإمارات ومئوية 2071 التي تسهم في تحقيق الجانب الوقائي في مكافحة الجريمة الإلكترونية، وجعل الإمارات أكثر البلدان أمناً على مستوى العالم، وفي ضوء المخاطر التي تهدد الأطفال أثناء استخدامهم الإنترنت، والتي قد يكون لها تداعيات اجتماعية عدة، حيث يمكن لضحايا الجرائم السيبرانية التي ترتكب عبر الفضاء

48 تقرير الإلكترونية في الشرق الأوسط لعام 2020 الذي أعدته مؤسسة سيرفس بلان الشرق الأوسط، مجلة الغرفة – غرفة تجارة وصناعة رأس الخيمة، العدد 348، يناير 2021، ص 21.

49 الموقع الإلكتروني لبوابة حكومة الإمارات: https://u.ae/ar-ae/about-the-ua تاريخ زيارة الموقع: 2024/7/05.

الإلكتروني والحواسيب والشبكات الإبلاغ عنها في دولة الإمارات العربية المتحدة عبر منصة e.Crime التابعة للقيادة العامة لشرطة دبي، أو عبر خدمة "أمان" التابعة للقيادة العامة لشرطة أبوظبي، أو عبر التطبيق الذكي "مجتمعي آمن"، حيث يلاحظ أن خدمة أمان هي إحدى أهم مبادرات شرطة أبوظبي تم إطلاقها في عام 2009 وذلك من أجل تعزيز الدور المجتمعي في الحفاظ على مجتمع آمن ومستقر، حيث تعد خدمة أمان قناة أمنية تعمل بحرفية عالية على مدار الساعة وطوال أيام السنة لتوفر للجمهور حرية الإدلاء بأي معلومة (أمنية– مجتمعية – مرورية – أخرى) تساهم في الحد من الجرائم واكتشافها، كما تضمن الحفاظ على سرية الشخص مقدم المعلومة في نشر الوعي وزيادة مستوى الأمن والأمان في دولة الإمارات العربية المتحدة.

المطلب الثاني: تسليم المجرمين في مجال الجرائم المعلوماتية

تثير الجرائم المرتكبة عبر الوسائل الإلكترونية العديد من الأشكال المتعلقة بضبط وإحضار المتهمين ما لم تكن السلوكيات من قبيل جرائم الإرهاب أو الجرائم الماسة بأمن الدولة، أو الجرائم الماسة بحقوق الملكية الفكرية وجرائم المخدرات والأسلحة وإباحة الأحداث، إذ أنه غالباً ما يتم اعتبار بقية أنماط الجرائم الإلكترونية من حيث الإجراءات المتبعة في ملاحقة وضبط الجناة من قبيل الجرائم التقليدية، بمعني آخر تطبق بشأنها ذات الإجراءات المتبعة في ملاحقة وضبط الجناة مرتكبي الجرائم التقليدية، لاسيما وأن هناك اختلاف في مفهوم بعض الجرائم، إذ ما يعد جريمة في دولة ما قد لا يعد كذلك في دولة أخرى، نظراً لاختلاف التقاليد والثقافات بمختلف أنواعها من مجتمع لآخر50، مثال على ذلك يختلف مفهوم السب والإساءة في الدول العربية عما هو عليه في الولايات المتحدة الأمريكية، فما يعتبر قذفاً في دولة الإمارات قد يعتبر من قبيل حرية الرأي والتعبير في أمريكا.

وعليه، فإن عدم وجود اتفاق دولي في تحديد تعريف المصطلحات الواردة في القوانين الجزائية خاصة تلك المعنية بمكافحة الجرائم الإلكترونية، يجعل من مسألة التعاون الدولي أمر مشوب بصعوبات بالغة، ما لم يكن هناك إطار عام لتحديد مسائل التعاون الدولي لهذا النمط من الجرائم، من بينها توحيد المفاهيم، وهذا أمر يكاد أن يكون مستحيلاً بالنسبة لبعض الجرائم – خاصة لما فيه من صعوبات تتعلق بآلية الضبط والتحقيق والمحاكمة، الأمر الذي يحتم على الدول إيجاد وسائل لمكافحة هذا النوع من الإجرام العابر للحدود من خلال تعزيز التعاون الدولي واتخاذ ما يلزم من تدابير وإجراءات تفعل هذا النمط من التعاون، لاسيما بشأن تسليم المجرمين.

ويعتبر تسليم المجرمين شكل من أشكال التعاون القضائي الدولي في مكافحة الجريمة، بل أهمها، خاصة في ظل تطور وسائل المواصلات والاتصالات بين الدول، إذ لم تعد الحدود القائمة بين الدول تشكل حاجزاً أمام مرتكبي

50 خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق، ص 45.

الجرائم، ولاعتبارات السيادة وعدم جواز التدخل في شؤون الدول وإجراءاتها متى كان الجاني هارباً كان لابد من إيجاد آلية للتعاون الدولي بشأن تسليم المجرمين[51].

ويقصد بالتسليم تخلى دولة عن متهم موجود على إقليمها إلى دولة أخرى بناء على طلبها لمحاكمته عن جريمة تعاقب عليها قوانينها، أو لتنفيذ فيه حكمها الصادر من محاكمها، وذلك بغرض عدم إفلات المتهم من العقاب[52]، كما يعرف بأنه إجراء تعاون دولي تقوم بمقتضاه دولة تسمى بالدولة الطالبة بتسليم شخص يوجد على إقليمها إلى دولة ثانية تسمى بالدولة المطالبة إليها أو جهة قضائية دولية بهدف ملاحقته عن جريمة اتهم بارتكابها أو لأجل تنفيذ حكم جنائي صدر ضده[53].

وفي إطار التعاون الدولي صادقت دولة الإمارات العربية المتحدة على العديد من الاتفاقيات الثنائية والدولية بشأن التعاون القضائي، كالاتفاقية العربية لمكافحة غسل الأموال وتمويل الإرهاب 2010م والاتفاقية العربية لمكافحة جرائم تقنية المعلومات 2010م، واتفاقية الرياض العربية للتعاون القضائي 1983م، واتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية "باليرموك 2000م"، كما صادقت على انضمامها إلى بروتوكول منع وقمع الاتجار بالأشخاص وبخاصة النساء والأطفال، المكمل لاتفاقية الأمم المتحدة لمكافحة الجرائم المنظمة عبر الوطنية "باليرموك 2000م، وذلك وفقاً لأحكام المرسوم بقانون اتحادي رقم (71) لسنة 2008م[54].

هذا بجانب وجود اتفاقية بودابست بشأن مكافحة جرائم الإنترنت لعام 2001 والتي تعد أول اتفاقية دولية شاملة تتعلق بجرائم الحاسب الآلي والجرائم المرتكبة عبر الإنترنت والمرتكبة عبر أجهزة تقنية المعلومات الأخرى، وتسعى هذه الاتفاقية إلى التعاون الدولي لمكافحة جرائم المعلوماتية ومحاولة الحد منها، كما تسعى إلى تحقيق وحدة التدابير التشريعية بين الدول الأوروبية والدول المنظمة للاتفاقية من غير الدول الأوروبية، وقد وقعت على هذه الاتفاقية والتي تتضمن (48) مادة قانونية، (26) دولة أوربية، إضافة إلى كندا واليابان وجنوب أفريقيا والولايات المتحدة الأمريكية وعلى الرغم من هذه الاتفاقية أوربية الأصل إلا أنها دولية النزعة، أي أنها مفتوحة للدول الأخرى لطلب الانضمام إليها[55].

وقد اشترط القانون الاتحادي رقم (39) لسنة 2006 بشأن التعاون القضائي الدولي في المسائل الجنائية لتسليم المطلوبين عدة شروط، وهي: أن تكون الجريمة المطلوب التسليم من أجلها معاقب عليها في كلا الدولتين طالبة التسليم والمطلوب منها التسليم، أي ازدواجية التجريم بأن "يكون الفعل سبب التسليم معاقباً عليه في قانون كل من الدولتين الطالبة والمطلوب إليها التسليم، عل أن تتم مراعاة الاتفاقية الدولية الثنائية التي لا تشترط ازدواجية

51 محمد أحمد حبحب، جرائم تقنية المعلومات في دولة الإمارات، مرجع سابق، ص 125.

52 لطيفة الجميلي، الوجيز في شرح قانون الإجراءات الجزائية الاتحادي، مرجع سابق، ص 145.

53 خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق، ص 65.

54 الموقع الرسمي لمكافحة غسل الأموال https://u.ae/ar-ae/information-and-services/business/combatting-money-laundering، تاريخ زيارة الموقع: 2024/7/05.

55 لطيفة الجميلي، الوجيز في شرح قانون الإجراءات الجزائية الاتحادي، مرجع سابق، ص 146.

التسليم، مع الأخذ بعين الاعتبار أنه لا يؤثر في التسليم اختلاف تكييف الجريمة –جنحة أو جناية– كما لا يؤثر اختلاف أركان الجريمة في التسليم، على أن تكون الجريمة معاقب عليها في الدولتين بعقوبة مقيدة للحرية لمدة لا تقل عن سنة أو بأية عقوبة أشد، فإذا كان الطلب متعلقاً بتنفيذ العقوبة فقط أي أنه تمت محاكمة الجاني في الدولة المطلوب منها التسليم، فإنه يشترط حتى تسلم المحكوم عليه ألا تقل المدة المتبقية دون تنفيذ عن ستة أشهر على أن يكون الحكم واجب التنفيذ، هذا مع الأخذ بعين الاعتبار أن نظام تسلم المجرمين أو المحكوم عليهم يركن إلى الاتفاقيات، الدولية الثنائية أو الجماعية وفقاً للضوابط والشروط الواردة فيها، إن المدد أو الشروط قد تختلف من اتفاقية لأخرى، أما في حالة تعدد الجرائم الواردة في طلب التسليم، فيكفي أن تكون واحدة على الأقل من بين تلك الجرائم معاقب عليها مدة لا تقل عن سنة في حال طلب تسليم متهم، أو متبقي على التنفيذ مدة لا تقل عن ستة أشهر في حال طلب تسليم المحكوم عليه[56].

هذا مع الأخذ بعين الاعتبار أن هناك حالات لا يجوز فيها التسليم وهي: إذا كان المطلوب تسليمه يحمل جنسية الدولة المطلوب منها التسليم كذلك الأمر بالنسبة اللاجئين السياسيين، وإذا كان القانون في الدولة يعقد الاختصاص للسلطات القضائية المختصة بشأن الجريمة المطلوب التسليم من أجلها، وفي حال كان موضوع طلب التسليم جريمة سياسية أو مرتبطة بجريمة سياسية، أو إذا كانت الجريمة تنحصر في الإخلال بواجبات عسكرية، كما لا يجوز التسليم متى توافرت أسباب جدية للاعتقاد بأن طلب التسليم أنما قد به ملاحقة أو معاقبة شخص ما لأسباب تتعلق بانتمائه العرقي أو الديني أو لجنسية أو لآرائه السياسية، أو أن يكون من شأن توافر أي من هذه الأسباب الإضرار بمركز هذا الشخص. كذلك لا يجوز تسليم الشخص متى سبق لطالبة التسليم أن اتخذت في مواجهة المطلوب تسليمه إجراءات التحقيق أو المحاكمة عن ذات الجريمة محل موضوع التسليم، كما لا يجوز تسليم من سبق محاكمته عن الجريمة المطلوب تسليمه من أجلها وحكم ببراءته أو إدانته واستوفى العقوبة المحكوم بها، أو في حالة صدر في شأن ذات الجريمة حكم بات من محاكم الدولة، أو في حالة انقضاء الدعوى الجزائية أو سقوط العقوبة بمضي المدة عند تقديم طلب التسليم.

كما لا يجوز التسليم متى كان المطلوب تسليمه قد تعرض أو يمكن أن يتعرض في الدولة طالبة التسليم للتعذيب أو معاملة غير إنسانية أو مهنية أو لعقوبة قاسية لا تتناسب والجريمة، أو في حالة عدم توفير الحد الأدنى له من الضمانات المقررة في قانون الإجراءات الجزائية، وتأكيداً على ذلك قضت المحكمة الاتحادية العليا "أن استخلاص القصد من طلب التسليم واحتمال تعرض المطلوب تسليمه لعقوبات قاسية ومهنية لا تتناسب مع الجريمة المطلوبة من أجل التسليم، هي من مسائل الواقع التي تستقل بها محكمة الموضوع بغير معقباً عليها من المحكمة الاتحادية العليا"[57].

---

56 المادة (4) من القانون الاتحادي رقم (39) لسنة 2006 بشأن التعاون القضائي الدولي في المسائل الجنائية.

57 حكم المحكمة الاتحادية العليا، الطعن رقم 233 لسنة 2015م جزائي، جلسة 2015/9/29م.

فإذا كان من يجوز تسليمه قيد التحقيق أو المحاكمة عن جريمة أخرى في الدولة، يتم حينها تأجيل التسليم إلى أن ينتهي التحقيق أو تنتهي المحاكمة بصدور حكم بات، أما المحكوم عليه فيتم تسليمه بعد تنفيذ العقوبة المحكوم بها، ومع ذلك يجوز تسليمه بصفة مؤقتة متى تعدت الدولة طالبة التنفيذ إعادة في أقرب وقت بمجرد صدور قرار بشأنه[58].

هذا مع ضرورة مراعاة إجراءات التسليم من حيث استيفاء طلب التسليم كافة البيانات[59]، وإحالة إدارة التعاون القضائي الدولي بوزارة العدل طلب التسليم للنائب العام والذي يقوم بعرض الأمر على محكمة الاستئناف المختصة للبت في قرار التسليم، ويمكن للنائب العام أو من يفوضه حين ورود طلب التسليم أن يأمر بالقبض على المطلوب تسليمه في حالة التخوف من هربه ما لم يكن محبوساً، كما للنائب العام أو من يفوضه أن يخلي سبيله بضمان شخصي أو مالي يقدره[60].

ويمكن استعجال التسليم[61] وذلك بقرار من وزير العدل بناء على عرض النائب العام إذا كان التسليم لدولة واحدة ووافق المطلوب تسليمه كتابة على ذلك[62]، فإذا كان هناك أمر قبض صادر على المطلوب تسليمه من جهة قضائية أجنبية، يجوز حينها للنائب العام أو لمن يفوضه وذلك في حالة، أن يأمر بحبس المطلوب تسليمه مؤقتاً لحين ورود طلب التسليم[63]. ويستتبع ذلك ضرورة عرض المطلوب تسليمه، على النيابة العامة المختصة خلال 48 ساعة من وقت القبض عليه، وعلى النيابة العامة إحاطته علماً بسبب القبض ومضمون الطلب والأدلة وكافة المستندات مع إثبات أقواله في المحضر، على أن يقوم النائب العام بإحالة طلب التسليم إلى محكمة الاستئناف المختصة خلال 15 يوماً من تاريخ نظره، مع تكليف المطلوب تسليمه بموعد الجلسة المحددة لنظر الطلب.

وتطبيقاً على موضوع الدراسة، بمراعاة شروط التسليم المجرمين وأحكام الاتفاقيات الدولية الجماعية أو الثنائية بشأن تسليم المجرمين، تعتبر بعض الجرائم المرتكبة عبر الوسائل الإلكترونية خارج نطاق تطبيق قانون

---

58 المادة (10) من القانون الاتحادي رقم (39) لسنة 2006 بشأن التعاون القضائي الدولي في المسائل الجنائية.

59 نصت المادة (11) من القانون الاتحادي رقم (39) لسنة 2006 بشأن التعاون القضائي الدولي في المسائل الجنائية على أنه: "يقدم طلب التسليم كتابة بالطريق الدبلوماسي ويحال إلى الإدارة المتخصصة، مصحوباً بالبيانات والوثائق التالية مترجمة إلى اللغة العربية، ومصدقاً عليها رسمياً من الجهات المختصة: 1. اسم وأوصاف الشخص المطلوب، وصور فوتوغرافية له إن وجدت، مع أية بيانات أخرى من الممكن أ تفيد في تحديد هويته وجنسيته ومحل إقامته. 2.نسخة من النص القانوني المنطبق على الجريمة، والعقوبة المقررة لها في الدولة الطالبة. 3. نسخة رسمية من محاضر التحقيق وأمر القبض الصادر من الجهة القضائية الأجنبية المختصة مبيناً فيه نوع الجريمة والأفعال المنسوبة للشخص المطلوب وزمان ومكان ارتكابها، وذلك إذا كان الطلب خاصاً بشخص قيد التحقيق. 4. نسخة رسمية من حكم الإدانة مبيناً فيها نوع الجريمة والأفعال المنسوبة للشخص المطلوب تسليمه والعقوبة المقتضي بها، وما يفيد أن الحكم واجب التنفيذ وذلك إذا كان الطلب خاصاً بشخص محكوم عليه".

60 المادة (15) من القانون الاتحادي رقم (39) لسنة 2006 بشأن التعاون القضائي الدولي في المسائل الجنائية.

61 المادة (13) من القانون الاتحادي رقم (39) لسنة 2006 بشأن التعاون القضائي الدولي في المسائل الجنائية.

62 نصت المادة (14) من القانون الاتحادي رقم (39) لسنة 2006 بشأن التعاون القضائي الدولي في المسائل الجنائية على أنه: "يجب أن تتضمن الموافقة الكتابية للمطلوب تسليمه جميع بياناته الشخصية وبيانات القضية المطلوب تسليمه من اجلها وأن التسليم قد تم بكامل اختياره وعن علم بنتائجه".

63 المادة (15) من القانون الاتحادي رقم (39) لسنة 2006 بشأن التعاون القضائي الدولي في المسائل الجنائية.

التعاون الدولي بشأن التسليم، ومنها جريمتي السب عبر الوسائل الإلكترونية أو أي وسيلة من وسائل تقنية المعلومات المنصوص عليها في المادة (43) من المرسوم بقانون اتحادي رقم (34) لسنة 2021 بشأن مكافحة الشائعات والجرائم الإلكترونية، كون المشرع يعاقب عليها بعقوبة مقيدة للحرية محدداً الحد الأدنى فيها، إلا أن هذا الحد الأدنى المحدد لها لا يمكن معه إعمال التسليم، كونه يقل عن شرط المدة المحددة للتسليم وهي ألا تقل مدة العقوبة السالبة للحرية عن سنة، بمعنى أن المشرع حدد الحد الأدنى لعقوبة تلك الجريمة بمدة تقل عن سنة، بالتالي فإن هذه جريمتي السب عبر الوسائل الإلكترونية تخرج من نطاق تطبيق أحكام قانون تسليم لمجرمين ما لم تنص الاتفاقيات الثنائية خلاف ذلك، حيث تكون العقوبة فيها الحبس والغرامة التي لا تقل عن مائة وخمسين ألف درهم ولا تزيد على خمسمائة ألف درهم أو بإحدى هاتين العقوبتين.

وفي ذلك قضت محكمة نقض أبوظبي بأن "طلب التسليم فقد شرطاً من شروط التسليم وهو أن يكون الفعل معاقباً عليه في الدولة المطلوب إليها التسليم بالحبس لمدة لا تقل عن سنة بما لا يجوز معه إجابة الجهة طالبة التسليم إلى طلبها بتسليم الطاعن إليها وإذ خالف القرار المطعون فيه هذا النظر وقضى بتسليم الطاعن رغم تخلف شرط من شروط التسليم المنصوص عليها بالمادة السابعة من القانون الاتحادي رقم (39) لسنة 2006م وهو ما لا يتعارض مع اتفاقية التعاون القضائي بين البلدين، فغنه يكون قد خالف القانون بما يعيبه ويوجب نقضه دون حاجة لبحث باقي أوجه الطعن"[64].

وباستقراء المرسوم بقانون اتحادي رقم (34) لسنة 2021 بشأن مكافحة الشائعات والجرائم الإلكترونية نجد أن المشرع الإماراتي قد نص صراحة في هذا المرسوم بقانون على تسليم المجرمين بشأن كل من ارتكب إحدى الجرائم الواردة به خارج الدولة، وبالتالي فإن المشرع الإماراتي يطبق أيضاً بشأن الجرائم الإلكترونية التشريع الخاص بالتعاون الدولي المتمثل في القانون الاتحادي رقم (39) لسنة 2006 بشأن التعاون القضائي الدولي في المسائل الجنائية، وإعمالاً لما صادقت عليه الدولة من اتفاقيات تعني بمكافحة هذا النمط من الجرائم، وأيضاً لمبدأ المعاملة بالمثل.

الخاتمة

ومن خلال مما سبق فإن إطار جرائم تقنية المعلومات ومنها جريمتي السب، فإن التفتيش يقع على القطع الصلبة وهو جهاز الحاسب الآلي والأجهزة المتصلة به والشبكة والبرامج أو المكونات المنطقية للحاسب الآلي من بيانات ومعلومات، والجدير بالذكر أن النتيجة التي تنتهي إليها إجراءات التفتيش في جرائم تقنية المعلومات هي ضبط وتحريز الأدلة المعلوماتية التي تم الحصول عليها حال الوصول إليها، وفي هذه الحالة يلزم اتخاذ إجراءات معلوماتية محددة لكي يمكن القيام بضبط الأدلة المعلوماتية، فلا تصلح الإجراءات المادية المعرفة للقيام بضبط الأدلة كما هو

64 حكم محكمة النقض بأبوظبي، الطعن رقم 153 لسنة 2018 جزائي، جلسة 2018/3/26م.

الشأن في العالم المادي، باستثناء عملية الفصل الضرورية واللازمة بين الحاسب وبين كل شخص ليس له علاقة بالقائمين على الدعوى الجزائية، وذلك خشية قيام المتهم أو من له علاقة أو مصلحة ما بتدمير الأدلة وإزالتها من الحاسب الآلي.

أن التعاون الأمني على المستوى العربي في مكافحة الجرائم الإلكترونية مطلب أساسي وضروري، حيث أن الأمن الداخلي والخارجي لكل دولة عربية مرتبط بالأمن العربي الجماعي، وأن الإخلال بالأمن الداخلي في أي دولة تتعدى آثاره بالضرورة إلى الإخلال بالاستقرار في كافة نواحي الحياة، مما يؤثر في النهاية على محصلة القوة الذاتية للدول العربية كافة، وعليه يجب أن تلتزم كل دولة عربية بتبني الإجراءات الضرورية من أجل تطبيق الالتزامات الواردة في الاتفاقية، وتقديم المساعدة والاتصالات الأمنية اللازمة لمكافحة جرائم تقنية المعلومات».

النتائج

1. يصعب على الأجهزة الشرطية في أي دولة القضاء على الجرائم الإلكترونية عابرة الحدود بمعزل عن الأجهزة الشرطية في الدول المختلفة، لأن جهاز الشرطة في هذه الدولة أو تلك يصعب عليه تعقب المجرمين ومتابعتهم إذا ما عبروا حدود الدولة، ولذلك فإن الحاجة ملحة إلى تعاون أجهزة الشرطة بين الدول وتنسيق العمل فيما بينها لضبط المجرمين المعلوماتيين، ومكافحة نشاط الإجرام المعلوماتي الذي يتجاوز حدود الدولة وتقديم المساعدة القضائية اللازمة لغايات لغاية التحقيق أو الإجراءات المتعلقة بجمع الأدلة في جرائم تقنية المعلومات.
2. تتسم الجرائم الإلكترونية ومنها جريمتي السب، بصعوبة اكتشافها وإثباتها، ويرجع ذلك إلى خصائص تقنية المعلومات ذاتها، وخاصة السرعة العالية التي ترتكب بها، وهو ما يسهل ارتكابها ويسهل طمس معالمها ومحو آثارها غير المرئية قبل اكتشافها، إذ يستطيع الجاني أن يرتكب الجريمة دون أن يترك وراءه أي أثر خارجي ملموس، وإذا كانت ثمة دليل على الإدانة فيستطيع الجاني تدميره في ثوانٍ معدودة، خاصة وأن هذا النوع من الجرائم يعتمد على الذكاء في ارتكابها، وأن المجرم المعلومات يتميز بالمهارة التقنية العالية والمعارف الفنية في مجال المعلوماتية وأنظمة وبرامج الحاسبات المتنوعة.
3. تختلف إجراءات المعاينة والتفتيش وضبط الأدلة في الجرائم الإلكترونية، ومنها جريمتي السب، عن الجرائم التقليدية، حيث يتطلب من المحققين ومأموري الضبط القضائي الإلمام والمعرفة الجيدة بالحاسب الآلي وبرامجه، وكذلك بالإنترنت وطبيعته وتشغيله ووسائل التواصل الاجتماعي، ومن هم الخبراء والفنيين المعلوماتيين المناسبين الذي يندبهم للكشف عن الأدلة الرقمية وتحديد قيمتها التدليلية في الإثبات الجنائي.

التوصيات

1) نوصي المشرع بالنص على إجراءات تفتيش الأجهزة الرقمية وضبط المعلومات التي تحتويها ومراقبتها أثناء انتقالها ما بين الشبكات المعلوماتية والأنظمة الحاسوبية، وذلك من خلال النص عليه في المرسوم بقانون اتحادي رقم (34) لسنة 2021 بشأن مكافحة الشائعات والجرائم الإلكترونية، والعمل على وضع نصوص تتعلق بمراحل الإثبات الجنائي بالأدلة العلمية الحديث، لكي تستوعب وسائل الإثبات الجنائي وإعطائها الحجية القانونية.

2) أهمية تبادل الخبرات للوقوف على أفضل الممارسات في طرق منع ومكافحة الجريمة وضبطها واستشراف ذلك في ظل التطور التقني والتكنولوجي في عصر الذكاء الاصطناعي، والاهتمام بإصدار دليل إرشادي يهتم بالأمن السيبراني على المستوى المحلي والإقليمي والدولي وبالمحتوى الذكي للبرامج والمساقات التعليمية، إلى جانب تطوير منظومة الإعداد الأكاديمي والتدريبي لاستشراف مستقبل الجريمة وإعداد سيناريوهات المواجهة المحتملة وتطوير البنية التحتية التقنية في المجال الأمني لمواجهة التحديات المستقبلية في مجال مكافحة الجريمة

3) نوصي باستحداث مختبر جنائي رقمي مختص بالأدلة والآثار المادية الناتجة عن الجرائم الإلكترونية، وذلك على مستوى القيادات الشرطية بوزارة الداخلية، مما يسهل مهمة استخراج وفحص الأدلة الرقمية وتقديمها بأفضل صورة أمام منصات العدالة.

4) تطوير البرامج والدورات التدريبية الخاصة بالبحث والتحري، لاسيما المتعلقة بجمع الأدلة الرقمية ومعايير استخراجها، كونها ذات طبيعة فنية وعلمية معقدة، ولمواكبة أعضاء الضبط القضائي وأجهزة التحقيق الجنائي كافة التطورات العلمية والفنية في الإثبات الجنائي، والتغلب على العقبات والمشكلات التي تواجههم في الحصول على الدليل الرقمي.

References

‘Abd al-Azīz Sālim al-Sanīdī. (2018). Al-Sīyāsah al-‘Aqābīyah li-l-Musharri‘ al-Imārātī fī Muwājahat al-Jarā'im al-Iliktrūnīyah fī Ẓill al-Marsūm al-Ittihādī Raqm 5 li-Sanat 2012 Bishān Muwājahat Jarā'im Taqnīyat al-Ma'lūmāt. *Mājistīr Ghayr Munshūrah*, Kullīyat al-Qānūn, Jāmi'at al-Imārāt al-‘Arabīyah al-Muttaḥidah.

Abd al-Karīm Khālid al-Radā'idah. (2015). Al-Jarā'im al-Mustahdathah wa Istrātījīyat Muwājahatihā. *Dār al-Ḥāmid li-l-Nashr*, ‘Ammān.

‘Abd Allāh Ḥusayn ‘Alī. (2012). Sariqat al-Ma‘lūmāt al-Mukhazanah fī al-Ḥāsūb al-‘Ālī. *Dār al-Nahḍah al-‘Arabīyah*, al-Qāhirah.

Aḥmad Sa‘d Muḥammad al-Ḥusaynī. (2018). Jarā'im al-I‘itibār ‘Abr Shabakat al-Intarnet Jārimatī al-Sabb wa al-Qadhf. *Majallat al-Buḥūth al-Qānūnīyah wa al-Shurṭīyah*, Akādīmīyat al-Shurṭah, al-Qāhirah, al-‘Adad (9), Mārīs.

Amīr Faraj Yūsuf. (2015). Jarā'im Taqnīyat al-Ma‘lūmāt fī Dawāl al-Khalīj al-‘Arabī wa al-Juhūd al-Duwalīyah wa al-Mahallīyah li-Mukāfaḥatihā. *Dār al-Kutub wa al-Dirāsāt al-‘Arabīyah*, al-Qāhirah.

Dīnā ‘Abd al-‘Azīz Fahmī. (2018). Al-Ḥimāyah al-Jinā'īyah min Isā'at Istikhdām Mawāqi‘ al-Tawāṣul al-Ijtimā‘ī. *Dār al-Nahḍah al-‘Arabīyah*, al-Qāhirah.

Ḥasan Muḥammad Ḥasanwah al-Ẓanḥānī. (2020). Al-Ḥimāyah al-Jinā'īyah li-l-Bayānāt al-Shakhṣīyah fī Muwājahat al-Jarā'im al-Iliktrūnīyah. *Risālat Mājistīr Ghayr Munshūrah*, Kullīyat al-Imām Mālik li-l-Sharī‘ah wa al-Qānūn, Dubayy.

Khālid Ḥāmid Muṣṭafā. (2017). Sharḥ Qānūn al-Ijra'āt al-Jazā'īyah li-Dawlat al-Imārāt al-‘Arabīyah al-Muttaḥidah. *Dār al-Fikr wa al-Qānūn*, al-Qāhirah.

Khālid Mamdūḥ Ibrāhīm. (2010). Fan al-Tahqīq al-Jinā'ī fī al-Jarā'im al-Iliktrūnīyah, Dirasah Mumārasah. *Dār al-Fikr al-Jāmi‘ī*, al-Iskandariyah.

Muhammad Bashīrī, Muhammad al-Hanā'ī. (2009). Al-Jarā'im al-Iliktrūnīyah wa Subul Muwājahatihā. *Markaz al-Buḥūth al-Amnīyah*, Abū Ẓabī.

Muhammad Ḥabḥab. (2016). Jarā'im Taqnīyat al-Ma‘lūmāt fī Dawlat al-Imārāt. *Dār al-Kitāb*, al-‘Ayn.

Muṣṭafā Muḥammad Mūsā. (2015). Dalīl al-Taharrī ‘Abr Shabakat al-Intarnet. *Dār al-Kutub al-Qānūnīyah*, al-Qāhirah.

Mamdūḥ al-Sabbkī. (1998). Ḥudūd Sulṭat Mā'āmūr al-Ḍabṭ al-Quḍā’ī fī al-Tahqīq. *Dār al-Nahḍah al-‘Arabīyah*, al-Qāhirah.

Mamdūḥ ‘Abd al-Ḥamīd. (2001). Al-Baḥth wa al-Tahqīq fī Jarā'im Istikhdām al-Kompiyūtar. *Dār al-Ḥuqūq li-l-Nashr*, al-Shārjah.

Sālim Ruwāẓān al-Mūsawī. (2012). Jarā'im al-Qadhf wa al-Sabb ‘Abr al-Qanawāt al-Fiḍā'īyah. *Munshūrāt al-Ḥalabī al-Ḥuqūqīyah*, Bayrūt.

Sulaymān al-‘Atībī. (2018). Dūr al-Taḥarrīyāt wa al-Baḥth al-Jinā'ī fī al-Kashf ‘an al-Jarā'im al-Iliktrūnīyah. *Aṭrūḥah Duktūrāh Ghayr Munshūrah*, Jāmi‘at Nā'if al-‘Arabīyah li-l-‘Ulūm al-Amnīyah, al-Riyāḍ.

‘Ādil Ibrāhīm Ismā‘īl. (2015). Mukāfaḥat Jarā'im al-Sabb wa al-Qadhf ‘Abr al-Intarnet. *Majallat Kullīyat al-Dirāsāt al-‘Ulūm al-‘Ālīah*, Akādīmīyat al-Shurṭah, al-Qāhirah, al-‘Adad 33, ‘Uktūbar.

‘Alā' al-Dīn Shaḥātah. (2007). Al-T‘āwun al-Duwalī fī Majāl Mukāfaḥat al-Jarīmah. *Dār al-Nahḍah al-‘Arabīyah*, al-Qāhirah.

Laṭīfah al-Jumaylī. (2013). Al-Wajīz fī Sharḥ Qānūn al-Ijra'āt al-Jazā'īyah al-Ittihādī. *al-Āfāq al-Mushriqah*, al-Shārjah.

Yāsir Muḥammad al-Kūmī. (2016). Dūr Marḥalat Jam‘ al-Istidlālāt fī al-Ḥadd min al-Jarā'im al-Ma‘lūmīyah. *Majallat al-Buḥūth al-Qānūnīyah wa al-Shurṭīyah*, Akādīmīyat al-Shurṭah, al-Qāhirah, al-Sanāh al-Rābi‘ah, al-‘Adad al-Sābi‘, Mārīs.

Muhammad ‘Abdullāh Ibrāhīm. (2016). Al-Muwājaha al-Amnīyah li-Jarā'im Shabakat al-Ma‘lūmāt al-Duwalīyah. *Aṭrūḥah Duktūrāh Ghayr Munshūrah*, Kullīyat al-Dirāsāt al-‘Ulūm al-‘Ālīah, Akādīmīyat al-Shurṭah, al-Qāhirah.

Taqrīr al-Iliktrūnīyah fī al-Sharq al-Awsaṭ li-‘Ām 2020. (2021). *Majallat al-Ghurfah* – Ghurfat Tijārati wa Ṣinā‘at Rās al-Khaimah, al-‘Adad 348, Yanāyir.