الفصل الرابع

الدليل الجنائي الرقمي ودوره في إثبات جريمة نشر الأخبار الكاذبة عبر وسائل التواصل الاجتماعي

التمهيد:

ترتكز قواعد الإثبات على إقامة الدليل على الواقعة التي يستند إليها، ويعد هو الوسيلة التي يتوصل بها صاحب الحق إلى إثباته وتقديمه إلى القضاء ليمكنه منه، ويحتل الدليل الجنائي مكان الصدارة في نظرية الإثبات باعتباره النتيجة التي تهدف إلى تحقيقها، والأساس المحرك لقواعد الإثبات الجنائي.

وبظهور جريمة نشر الأخبار الكاذبة عبر وسائل التواصل الاجتماعي برز الدليل الرقمي من أدلة الإثبات لها، ويشمل مصطلح الدليل الرقمي كافة البيانات الرقمية التي من شأنها تأكيد ارتكاب الجريمة أو تأكيد وجود علاقة بين الجريمة والمجني عليه والمتهم، ويتبوأ مكان الصدارة لإقامة الدليل على الوقائع المرتكبة في البيئة الرقمية لنظم الحاسب الآلي وقواعد نظم الاتصال بالإنترنت.

وللتعرف على الدليل الجنائي الرقمي ودوره في إثبات جريمة نشر الأخبار الكاذبة عبر وسائل التواصل الاجتماعي، سيتم تقسيم هذا الفصل إلى مباحث ثلاثة، وذلك وفقًا للآتي:

المبحث الأول: مفهوم الدليل الرقمي وخصوصية جريمة نشر الأخبار الكاذبة عبر وسائل التواصل الاجتماعي

تهدف محاولات تعريف الدليل الرقمي للوصول لتوصيف دقيق يحدد أبعاده ومعناه، كما ينبغي وضعه في تصنيفه المناسب من أدلة الإثبات الجنائي، حيث ينعكس ذلك بالضرورة على مباشرة جهات البحث للتعامل مع الوقائع الرقمية واستخلاصه من مسرح الجريمة.

وللتعرف على مفهوم الدليل الرقمي وخصوصية جريمة نشر الأخبار الكاذبة عبر وسائل التواصل الاجتماعي، سيتم تقسيم هذا المبحث إلى مطالب ثلاثة، كالآتي:

المطلب الأول: مفهوم الدليل الرقمي

لتعريف الدليل الرقمي، لابد أولًا من التطرق إلى الدليل بصفةٍ عامة، وهذا بهدف التعرف على مفهوم الدليل الرقمي، وذلك لأنه من المنطقي وجوب دراسة الأصل العام المتمثل في الدليل بصفةٍ عامة، ثم التطرق إلى الفرع المتمثل في الدليل الرقمي. وعليه سنتناول في هذا المطلب معنى الدليل بوجهٍ عام، من خلال تعريفه لغةً، وكذا المعنى الاصطلاحي، وذلك كالآتي:

أولًا: الدليل في اللغة:

عُرف الدليل لغةً بأنه المرشد، وجاء في مختار الصحاح أن الدليل ما يستدل به، وهو الدال أيضًا وقد (دله) على الطريق يده بالضم، و(دلالة) بفتح الدال وكسرها و(دلولة) بالضم والفتح أعلى، ويقال: فلان (يدل) بفلان أي يثق به [195].

(195) صليبا. جميل. (2008). *المعجم الفلسفي*. لبنان: دار الكتاب اللبناني. ص 71.

ثانيًا: الدليل في الاصطلاح القانوني:

عُرف الدليل بأنه "الوقائع المادية أو المعنوية التي تتصل بالجريمة ويؤدي اكتشافها إلى تحيد كل أو بعض أبعاد الجريمة مثل: وقتها ومكانها ودوافعها، وأسلوب ارتكابها والظروف المحيطة بها ومسئولية أطرافها من متهمين ومجنى عليهم" (196).

وعُرف أيضًا بأنه "الوقائع المادية أو المعنوية التي تتصل بالجريمة، ويؤدي اكتشافها إلى تحديد كل أو بعض أبعاد الجريمة مثل وقتها ومكانها ودوافعها وأسلوب ارتكابها والظروف المحيطة بها، ومسئولية أطرافها من متهمين ومجني عليهم، ويؤدي تجميع روابط ما تسفر عنه من حقائق إلى تحديد مرتكب الجريمة بصورة قاطعة لا لبس فيها"(197).

وعرفه آخرون بأنه "البرهان القائم على المنطق والعقل، وفي إطار من الشرعية الإجرائية لإثبات صحة افتراض، أو لرفع أو خفض درجة اليقين الإقناعية في واقعة محل خلاف"(198).

كما عرفه آخرون بأنه "الحجية التي تستخلص من واقعة أو ظاهرة مادية أو معنوية متعلقة بالجريمة، بحيث يولد ظهورها الاقتناع الكافي بوقوع الجريمة، أو واقعة من وقائعها، وإسنادها إلى المتهم، أو نفي ذلك، وهو الوسيلة الإثباتية المشروعة التي تسهم في تحقيق حالة اليقين لدى القاضي بطريقة سائغة يطمئن إليها، وأن تؤدي عقلًا إلى ما رتبه عليها من أحكام" (199).

فالدليل الجنائي إذا هو الوسيلة الواقعة التي يقصد منها إرشاد القاضي الجنائي بأن الجريمة قام بها المتهم، وبه يكون ثمة إثبات، وعلى ذلك فالدليل الجنائي كل وسيلة مرخص بها أو مسموح بها قانونًا

(196) يوسف. أمير فرج. (2016). *الإثبات الجنائي للجريمة الإلكترونية والاختصاص القضائي بها*. مصر: مكتبة الوفاء القانونية. ص18.

(197) الصغير. أسامة (2007). *البصمات "وسائل فحصها وحجتها في الإثبات الجنائي"*. مصر: دار الفكر والقانون. ص 9.

(198) أبو القاسم. أحمد (2008). *الدليل الجنائي المادي ودوره في إثبات جرائم الحدود والقصاص*. السعودية: المركز العربي للدراسات الأمنية: أكاديمية نايف العربية للعلوم الأمنية. ص184.

(199) البقمي. ناصر بن محمد (2012). " أهمية الأدلة الرقمية في الإثبات الجنائي. دراسة وفق الأنظمة السعودية". ***مجلة الفكر الشرطي***. الإمارات. المجلد 21. العدد 80. ص23.

لإثبات وجود أو عدم وجود الواقعة المرتكبة أو صحة أو كذب وقوعها. أي أنه الدليل المطلوب للإثبات الجنائي لكي يكون ثمة فصل في الدعوى الجنائية بالبراءة والإدانة [200].

ويرى الباحث يمكن استخلاص من التعريفات السابقة أن الدليل الجنائي هو التي تستعين بها أجهزة العدالة في كشف الحقيقة، عن طريق تأكيد الاتهام أو نفيه.

ثالثًا: تعريف الدليل الرقمي:

نظرًا للطبيعة الخاصة للجرائم المتصلة بالتكنولوجيا الحديثة سواء الجرائم الإلكترونية أو الجرائم المستحدثة (التقليدية والمعتمدة على التكنولوجيا) فطريقة إثباتها بالأدلة التقليدية مثل الكتابة والشهادة وغيرها يكاد يكون مستحيلًا، فلا يتصور أن يقول شخص أنه رأى آخر يخترق موقعًا مثلًا على حاسوبه، فتلك الجرائم تحتاج لنوعية خاصة من الأدلة تستخدم فيها الطبيعة التقنية الناجمة عن أجهزة الحاسوب، والتي تتمثل في الأدلة الإلكترونية، وبمعنى آخر تقوم عملية الإثبات الجنائي في جريمة نشر الأخبار الكاذبة عبر وسائل التواصل الاجتماعي على الدليل الإلكتروني، إذ يعد الوسيلة الوحيدة لإثبات تلك الجرائم. وللتعرف على مفهوم الدليل الرقمي يقوم الباحث باستعراض هذه التعريفات من خلال ما يلي:

لقد استخدم مصطلح الدليل الرقمي [201] من قبل المشرع الأوروبي في التوصية رقم (13/95) الخاصة بمشكلات الإجراءات الجنائية المتعلقة بتكنولوجيا المعلومات [202]، كذلك تم استعماله في الفقرة

---

(200) عزت. فتحي محمد أنور (2010). *الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية*. مصر: دار الفكر والقانون. ص66.

(201) إن أصل مصطلح الرقمية يرجع إلى استخدام النظام الرقمي الثاني (1000) وهي الصيغة التي تسجل بها البيانات (أشكال وحروف ورموز وغيرها) داخل الحاسب الآلي، حيث يمثل الصفر (0) وضع الإغلاق OFF والواحد (1) وضع التشغيل (ON)، ويعرف الرقم (0) أو (1) بالبيت BIT، ويشكل عدد 8 BIT ما يعرف بالبيت BIT.
فرغلي. عبد الناصر محمد محمود؛ المسماري. محمد عبيد سعيد. (2007). "الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والرقمية". ***المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي***. السعودية: جامعة نايف العربية للعلوم الأمنية. ص11.

(202) توصيات لجنة وزراء المجلس الأوروبي. التوصية رقم 95 بند 13. المعتمدة بتاريه 1995/11/23.

الثانية من المادة (14) من اتفاقية بودابست [203]، كما جاء هذا الوصف أيضًا في المرشد الفيدرالي الأمريكي لتفتيش وضبط الحاسب في التحقيقات الجنائية [204].

ويعرف الدليل الرقمي بأنه "معلومات يقبلها المنطق والعقل ويعتمدها العلم، يتم الحصول عليها بإجراءات قانونية وعلمية، بترجمة البيانات الحسابية المخزنة في أجهزة الحاسب الآلي وملحقاتها وشبكات الاتصال، ويمكن استخدامها في أي مرحلة من مراحل التحقيق أو المحاكمة لإثبات حقيقة فعل أو شئ أو شخص له علاقة بجريمة أو جان أو مجني عليه"[205].

وعرفه آخرون بأنه "الدليل المأخوذ من أجهزة الحاسب الآلي، ويكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية، ممكن تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة، ويتم تقديمها في شكل دليل يمكن اعتماده أمام القضاء. وهو مكون رقمي لتقديم معلومات في أشكال متنوعة، ومن ذلك: النصوص المكتوبة والصور والأصوات والأشكال والرسوم، وذلك من أجل الربط بين الجريمة والمجرم والمجني عليه وبشكل قانوني يمكن الأخذ به أمام أجهزة إنفاذ وتطبيق القانون"[206].

وعرف أيضًا بأنه " مكون رقمي لتقديم معلومات في أشكال متنوعة ومن ذلك: النصوص المكتوبة أو الصور والأصوات والأشكال والرسوم، وذلك من أجل الربط بين الجريمة والمجرم والمجني عليه وبشكل قانوني يمكن الأخذ به أمام أجهزة إنفاذ وتطبيق القانون"[207]. كما عرف بأنه " الدليل المستمد من وسائط ترتبط بتقنية المعلومات، وكلها تدور حول استخدامات الحاسب الآلي وتطبيقاته، وشبكة

---

(203) شهدت العاصمة المجرية بودابست أولى المعاهدات الدولية التي تكافح الجرائم المعلوماتية في 2001/2311، حيث وقع عليها ثلاثون دولة بما في ذلك الدول الأربع من غير الأعضاء في المجلس الأوروبي وهي كندا واليابان وجنوب أفريقيا وأمريكا.

(204) بن يونس. عمر محمد. (2009). *الإجراءات الجنائية عبر الإنترنت المرشد الفيدرالي الأمريكي لتفتيش وضبط الحواسيب وصولًا إلى الدليل الإلكتروني في التحقيقات الجنائية*. مصر: الدار الجامعية للنشر. ص9.

(205) البشري. محمد الأمين (2008). *التحقيق في الجرائم المستحدثة*. الرياض: أكاديمية نايف العربية للعلوم الأمنية. ص234.

(206) عبد المطلب. ممدوح (2006). *البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت*. مصر: دار الكتب القانونية. ص88.

(207) عرف القانون رقم (5) لسنة 2012م في شأن مكافحة جرائم تقنية المعلومات بدولة الإمارات في المادة الأولى منه: البرنامج المعلوماتي: "مجموعة من البيانات والتعليمات والأوامر. قابلة للتنفيذ بوسائل تقنية المعلومات والمعدة لإنجاز مهمة معينة".

"الإنترنت" وغيرها من التقنيات الحديثة، ويتعلق بالطبع بجريمة معلوماتية، إذا فالدليل المعلوماتي يتعلق بجريمة معلوماتية، وهي جرائم الكمبيوتر والإنترنت، والتجارة الإلكترونية [208].

ومن التعريفات الشهيرة للدليل الرقمي تعريف الفقيه (كاسي Casey) بأنه "جميع البيانات الرقمية التي يمكن أن تثبت أن هناك جريمة قد ارتكبت، أو توجد علاقة بين الجريمة والجاني، أو توجد علاقة بين الجريمة والمتضرر منها؛ والبيانات الرقمية في مجموعة الأرقام التي تمثل مختلف النصوص بما فيها النصوص المكتوبة، الرسومات، الخرائط، الصوت والصورة"[209].

كما عرفه البعض بأنه "الوسيلة الرئيسية والوحيدة لإثبات الفعل غير المشروع الواقع عبر جهاز الحاسب الآلي، من خلال أخذ الدليل عن طريق جهاز الحاسب الآلي في شكل مجالات مغناطيسية أو نبضات كهربائية، يمكن تجميعها وتحليلها باستخدام برامج وتطبيقات خاصة، تشكل في نهاية الأمر بصمة رقمية، ويتم تقديمها في شكل دليل يمكن اعتماده أمام القضاء"[210].

وعرفته المنظمة الدولية لأدلة الحاسب الآلي (IOCE) بأنه "المعلومات المخزنة أو المتنقلة في شكل ثنائي، والتي يمكن الاعتماد عليها أمام المحكمة"[211].

ومما سبق نجد أن الدليل الرقمي ذات طبيعة ديناميكية فائقة السرعة تنتقل من مكان لآخر عبر شبكات الاتصال من خلال وسائل التواصل الاجتماعي متعدية لحدود الزمان والمكان، ويبدو أن الدليل الرقمي يعتمد على التطور التلقائي وهذا راجع إلى البيئة التقنية المتطورة بطبيعتها، ومن خلال الدليل الرقمي يمكن رصد المعلومات عن الجاني وتحليلها في ذات الوقت.

---

(208) حجازي. عبد الفتاح بيومي (2009). *الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية*. مصر: دار النهضة العربية. ص709.

(209) عزت. فتحي محمد (2010). *الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية*. ص78.

الجملي. طارق محمد (2015). "الدليل الرقمي في مجال الإثبات الجنائي". ***مجلة الحقوق المجلد***. رقم 12. العدد رقم 1. كلية الحقوق. جامعة البحرين. ص19.

(210) صالح. العيد يسن مكي (2016). *حجية الدليل الرقمي في الإثبات*. السودان : دار عزة للنشر والتوزيع.. ص80.

(211) عزت. فتحي محمد أنور (2010). *الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية*. ص684.

وفي هذا السياق يعرف الباحث الدليل الرقمي بأنه: "الدليل المستخلص من أو بواسطة وسائل التقنية الحديثة، لتقديمها للقضاء بعد تفسيرها في شكل مقروء أو مكتوب أو مرسوم أو مصور، بواسطة طرق قانونية وفنية لإثبات وقوع الجريمة ولتقرير البراءة أو الإدانة فيها".

المطلب الثاني: خصوصية جريمة نشر الأخبار الكاذبة عبر وسائل التواصل الاجتماعي

1- خفاء الجريمة:

تتصف جريمة نشر الأخبار الكاذبة عبر وسائل التواصل الاجتماعي بأنها خفية مستترة في أغلبها، فالمجني عليه غالبًا لا يلحظها، مع أنها قد تحدث أثناء اتصاله بالشبكة، ولكن لا يعلم بها ولا ينتبه إليها، إلا بعد فترة من وقوعها، وأحيانًا أخرى لا يكتشف أمرها، ويرجع ذلك إلى تعامل الجاني مع نبضات إلكترونية غير مرئية، لا يمكن قراءتها إلا بواسطة الحاسب، إضافة إلى أن توافر المعرفة، والخبرة الفنية لدى الجاني في هذا المجال يؤدي إلى صعوبة اكتشاف جريمته، وذلك باتباعه لأساليب لا ينتبه إليها المستخدم العادي للشبكة، ومن أمثلتها إرسال الفيروسات المدمرة، وسرقة الأموال والبيانات الخاصة، أو إتلافها، والتجسس وغيرها من الجرائم، ثم يقوم بدس بعض البرامج الخاصة وتغذيتها ببعض البيانات التي تؤدي إلى عدم شعور المجني عليه بوقوع هذه الجرائم[212].

2- سرعة التطور في ارتكاب الجريمة:

التطور المتسارع الذي تشهده تكنولوجيا المعلومات، أرخى بظلاله على جريمة نشر الأخبار الكاذبة عبر وسائل التواصل الاجتماعي، حيث إن أساليب ارتكابها في تطور مستمر دائما، وأن المجرمين في جميع أرجاء العالم يستفيدون من الشبكة في تبادل الأفكار، والخبرات الإجرامية فيما بينهم.

(212) الكعبي. محمد عبيد (2009). *الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت*. مصر: دار النهضة العربية. ص33.

3– جريمة أقل عنفًا في التنفيذ:

لا تحتاج جريمة نشر الأخبار الكاذبة عبر وسائل التواصل الاجتماعي إلى عنف عند تنفيذها، أو مجهود كبير، وإنما تنفذ بأقل جهد ممكن يقوم به الجاني، ويعتمد فيها بصورة رئيسية على الخبرة في المجال المعلوماتي، وهذا على خلاف الجرائم التقليدية التي يستخدم فيها عنف، وتراق فيها الدماء، ويقوم الجاني بمجهود كبير به غالبًا في الوصول إلى غايته.

4– جريمة عابرة الحدود:

إن تقنية استخدام وسائل التواصل الاجتماعي من خلال شبكة "الإنترنت" ألغت الحدود الجغرافية بين مختلف دول العالم ولم تعد الجريمة تخضع لنطاق إقليمي محدود، وإنما أصبحت الجريمة يتم التخطيط لها في بلد وتمر عبر بلد آخر وتتحقق نتيجتها في بلد ثالث أو عدة بلدان في ثوان معدودة، هذا وقد لا يقع الضرر المترتب على الجريمة على المجني عليه وحده وإنما قد يتعداه إلى متضررين آخرين في دول عدة، وهذا هو الذى نلاحظه من خلال جريمة نشر الأخبار الكاذبة عبر وسائل التواصل الاجتماعي من حيث الخطر الديني أو الأخلاقي أو الأمني أو السياسي أو الثقافي أو التربوي أو الاقتصادي[213].

5– انعدام الآثار التقليدية للجريمة:

نجد في الجريمة التقليدية أن أغلب المجرمين يتركون أثرًا يؤدي إلى اكتشافهم والقبض عليهم ولو بعد فترة من الزمن، أما في حالة جريمة نشر الأخبار الكاذبة عبر وسائل التواصل الاجتماعي فلا يمكن العثور في أغلب الأحيان على آثار خارجية أو مادية توصل إلى مرتكبها.

(213) الجنبيهي، منير محمد والجنبيهي، ممدوح محمد (2013). *جرائم الإنترنت والحاسب الآلى ووسائل مكافحتها*. مصر: دار الفكر الجامعى. ص14.

6- سرعة غياب الدليل المرئي والصعوبة في إثباته:

تكون البيانات والمعلومات المتداولة عبر شبكة "الإنترنت" على هيئة رموز مخزنة على وسائط تخزين ممغنطة ولا تقرأ إلا بواسطة الحاسب الآلي، والعثور على الدليل الذي يمكن فهمه بالقراءة والتوصل عن طريقه إلى الجاني يبدو أمرًا صعبًا لاسيما وأن الجاني يحرص على عدم ترك أثرًا لجريمته، أضف إلى ذلك ما يتطلبه من فحص دقيق لموقع الجريمة عن طريق مختصين في هذا المجال للعثور على ثمة دليل ضد الجاني، وما يلي ذلك من فحص للكم الكبير من الوثائق والمعلومات والبيانات المخزنة، إضافة إلى ما يتطلبه ذلك من تكلفة اقتصادية عالية في ضوء غياب الخبرة الكافية لدى الأجهزة الأمنية والقضائية.

7- إحجام المجني عليهم عن الإبلاغ:

عند وقوع جريمة نشر الأخبار الكاذبة عبر وسائل التواصل الاجتماعي نجد أن بعض المجني عليهم يحجمون عن إبلاغ السلطات المختصة خوفًا على السمعة والمكانة وعدم هز الثقة في الكفاءة، ومحاولة إخفاء طريقة ارتكاب الجريمة حتى لا يتم تقليدها من جانب الآخرين، مما يشجع الجناة على ارتكاب مزيد من تلك الأفعال التي تشكل الجريمة، وقد أدى ذلك إلى اقتراح البعض في الولايات المتحدة الأمريكية بأن تلزم النصوص المتعلقة بجرائم الحاسبات موظفي الجهة المجني عليها بالإبلاغ عما يقع عليها من جرائم في هذا المجال متى وصل إلى علمهم مع وضع جزاء في حالة إخلالهم بهذا الالتزام[214].

8- نقص الخبرة لدى الأجهزة الأمنية والقضائية:

يتطلب اكتشاف جريمة نشر الأخبار الكاذبة عبر وسائل التواصل الاجتماعي إلمامًا بالأمور الفنية والتقنية لدى أجهزة الشرطة والنيابة العامة والقضاء من أجل التوصل إلى مرتكبي هذه الجرائم وإثباتها ويستلزم ذلك أسلوبًا خاصًا في التحقيق والتعامل مع مثل هذه الجرائم ذات التقنية المتطورة والأساليب المعقدة،

(214) الجنبيهي، منير محمد والجنبيهي، ممدوح محمد (2013). *جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها*. ص16.

الأمر الذي وجدت معه هذه الأجهزة أنها غير قادرة على التعامل مع هذا النوع من الجرائم، ولجأت بعض الدول إلى الاستعانة ببعض المجرمين الذين يطلق عليهم مصطلح "الهاكرز" (Hackers) للتوصل إلى كشف غموض بعض جرائم الإنترنت وإنشاء مراكز متخصصة لهذا الغرض[215].

9- سهولة إتلاف وتدمير الدليل المادي:

من السهولة على المجرم في جريمة نشر الأخبار الكاذبة عبر وسائل التواصل الاجتماعي طمس الدليل في وقت قياسي، ولا يستغرق ذلك سوى ثوان معدودة وذلك بالاستعانة بالبرامج المخصصة لذلك [216].

10- إعاقة الوصول إلى الدليل بوسائل الحماية الفنية:

يحاول المجرم في جريمة نشر الأخبار الكاذبة عبر وسائل التواصل الاجتماعي قدر الإمكان إعاقة الوصول إليه بشتى الطرق، فهو بعد ارتكاب جريمته يقوم بدس برامج أو وضع كلمات سرية ورموز تعوق الوصول إلى الدليل، كما يلجأ إلى تشفير التعليمات مما يصعب من عملية الوصول إلى ثمة دليل يدينه[217].

ويرى الباحث أنه نظرًا لما تستلزمه هذه الجرائم من تقنية لارتكابها فهي تتطلب لاكتشافها والبحث عنها أسلوبًا خاصًا في التحقيق والتعامل، الأمر الذي لا يوجد في الجهات الأمنية والقضائية في معظم البلدان، نظرًا لنقص المعارف التقنية، مما يتطلب تخصصًا في التقنية لتحصين الجهاز الأمني والقضائي ضد هذه الظاهرة.

(215) الهاكرز أو القرصان هو شخص خبير بلغة البرمجة ويستطيع الدخول على غيره والتجسس عليهم، وأول ما ظهر في عام 1984 عندما استطاع ليكر لوثر إنشاء مجموعة من القراصنة يقومون بالدخول على أجهزة الآخرين، ثم ظهرت عام 1990 مجموعة أخرى قامت لمنافستهم ومحاولة كل طرف اختراق الآخر حتى سميت حرب الهاكرز العظمى واستمرت أربع سنوات انتهت بإلقاء القبض على بعضهم، وبعد كيفن ميتيلك أشهر هاكر في التاريخ استطاع اختراق كمبيوتر الشركة التي يعمل بها وسجن عام وخرج أكثر ذكاء ومارس هوايته.

(216) عثمان. حازم محمد حنفي (2016). ***الدليل الإلكتروني ودوره في المجال الجنائي***. (رسالة دكتوراه). مصر: جامعة القاهرة. ص235.

(217) المصدر نفسه. ص237.

المطلب الثالث: أحكام الأدلة الرقمية المتحصلة من جريمة نشر الأخبار الكاذبة عبر وسائل التواصل الاجتماعي

الأصل في إجراءات المحاكمة هو أن تكون المرافعة شفوية وحضورية ويقصد بالمرافعة هنا كل إجراءات التحقيق النهائي الذي تجريه المحكمة، ومفهوم مبدأ وجوب مناقشة الدليل الرقمى يعنى بصفة عامة أن القاضي لا يمكن أن يؤسس اقتناعه إلا على العناصر الإثباتية التي طرحت في جلسات المحاكمة وخضعت لحرية مناقشة أطراف الدعوي ولا يختلف الأمر بالنسبة للأدلة الرقمية بوصفها أدلة إثبات حيث يجب أن تطرح في الجلسة وأن يتم مناقشتها في مواجهة أطراف الدعوي.

وتأسيسًا على ذلك فإن الأدلة الرقمية سواء كانت مطبوعة أو بيانات معروضة على شاشة الحاسب الآلي أو كانت بيانات مدرجة في حاملات البيانات فإنه يجب مناقشتها وتحليلها، كما أن قاعدة وجوب مناقشة الدليل الجزائي سواء كان دليل تقليدي أم كان ناتجة عن الحاسب الآلي تعد ضمانات مهمة وأكيدة للعدالة حتى لا يحكم القاضي الجزائي في الجرائم المعلوماتية الشخصية أو بناء على رأي الغير [218].

وبناء على ذلك نجد أن المشرع الإماراتي أوجب ضرورة مناقشة الدليل الوارد بملف الدعوى، فوفقًا لنص المادة (209) من قانون الإجراءات الجزائية الاتحادي يمكن أن نجد ما يلي:

أولًا: ورود الدليل بملف الدعوى:

فمن خلال نص المادة (209) سالف الإشارة إليها، يُستنتج أن الدليل الرقمي يجب أن يكون له أصل في أوراق الدعوى المطروحة على القاضي، حتى يستطيع القاضي أن يبني عليه حُكمه؛ فالدليل الذي لا

(218) عثمان. حازم محمد حنفي (2016). ***الدليل الإلكتروني ودوره في المجال الجنائي***. ص238.

يتحقق فيه هذا الشرط يكون منعدمًا في نظر القانون، وذلك إعمالًا لقاعدة وجوب كتابة جميع إجراءات الاستدلال والتحقيق [219].

فدليل الإثبات الصحيح يجب أن يكون له أصل في أوراق الدعوى المطروحة على القاضي حتى يمكن للقاضي أن يبنى عليه حكمه، فالدليل الذي لا يتحقق فيه هذا الشرط يكون منعدمًا في نظر القانون، وذلك استنادًا إلى قاعدة وجوب تدوين كافة إجراءات الاستدلال والتحقيق [220].

وهذا ما أكدته المحكمة الاتحادية العليا الإماراتية حينما قضت بأنه: "لقضاة الموضوع السلطة المطلقة في تقدير أدلة الإثبات بدون معقب ما دام ما استندوا إليه له أصل ثابت في أوراق الدعوى" [221]. كما قضت أيضًا بأنه: "يجوز لقضاة الاستئناف أن يأخذوا بالدليل الذي يرونه صالحًا لتدعيم اقتناعهم على شرط أن يكون له أصل ثابت بأوراق الدعوى وأن يعللوا قضاءهم تعليلًا كافيا".

ثانيًا: وجوب طرح الدليل الرقمي في الجلسة وحصول المناقشة فيه:

يقصد بقاعدة وجوب مناقشة الدليل، خضوعه لحرية مناقشة أطراف الدعوى إعمالًا لمبادئ المحاكمة الجنائية، المتمثلة في الشفوية والعلنية [222]. فالقاضي يحكم في الدعوى حسب العقيدة التي تكونت لديه بكامل حريته وفقًا لمبدأ الاقتناع الشخصي، إلا أنه مقيد بأن تكون الأدلة التي كونت عقيدته معروضة على بساط البحث في الجلسة، حتى يتمكن أطراف الدعوى من الاطلاع عليها وإبداء آراءهم فيها[223]، فعلى القاضي إذا أن يطرح للمناقشة كل دليل قدم فيها حتى يكون الخصوم على بينة مما

(219) محمد. فاضل زيدان (2006). *سلطات القاضي الجنائي في تقدير الادلة* "دراسة مقارنة". الأردن: دار الثقافة للنشر والتوزيع. ص248.

(220) الجابري. إيمان محمد علي (2005). *يقين القاضي الجنائي*: دراسة مقارنة، مصر: منشأة المعارف. ص139.

(221) بغدادي. جيلالي (1996). *الاجتهاد القضائي في المواد الجنائية*. الجزائر: الديوان الوطني للأشغال التربوية. الجزء الأول. ص16.

(222) مروان. محمد (2004). "المبادئ الأساسية التي تحكم نظام الإثبات في المسائل الجنائية في قانون الإجراءات الجزائية الجزائري"، ***مجلة الدراسات القانونية***. لبنان: ع1. ص ص58- 59.

(223) مستاري. عادل (2008). "دور القاضي الجنائي في ظل مبدأ الاقتناع القضائي". ***مجلة المنتدى القانوني***. الجزائر: جامعة محمد خيضر. ع 5. ص188.

تقدم ضدهم من أدلة، ومن ثم يصبح الحكم باطلًا إذا كان مبناه دليلًا لم يطرح للمناقشة، أو لم تتح للخصوم فرصة إبداء الرأي فيه، أو إذا لم يعلموا به أصلًا وليس له أيضًا الاعتماد على أدلة يستمدها من دعوى أخرى لم يقرر ضمها إلى الدعوى المنظورة أمامه[224]. وتترتب نتيجتان مهمتان على قاعدة وجوب طرح الدليل في الجلسة وحصول المناقشة فيه وهما:

1– عدم جواز أن يقضي القاضي بناءً على معلومات شخصية:

ففكرة عدم جواز أن يقوم القاضي بالقضاء في جريمة نشر الأخبار الكاذبة عبر وسائل التواصل الاجتماعي بناء على معلوماته الشخصية من أهم النتائج المترتبة على قاعدة وجوب مناقشة أو طرح الدليل الجنائي سواء كان دليلًا تقليديًا أم رقميًا في الجلسة لأنه لا يجوز للقاضي أن يحكم بمقتضي معلوماته الشخصية في الدعوى أو على ما رآه بنفسه أو حققه في مجلس القضاء وبدون حضور الخصوم لأن هذه المعلومات لم تعرض في الجلسة، ولم تتم مناقشتها وتقييمها ومن ثم يصبح الاعتماد عليها مناقضا لقاعدتي الشفوية والمواجهة التي تسود مرحلة المحاكمة[225]، كذلك فإن هناك تناقضا بين صفتي القاضي والشاهد إذ أن الشهادة تستلزم إدراك الوقائع ثم نقلها إلى حيز الدعوى وفي هذه العملية تتدخل اعتبارات عدة منها عنصر التقدير لدى الشاهد وإدراكه وذاكرته إلى غير ذلك من العوامل والمؤثرات التي لها دخل كبير في تقدير الشهادة ولهذا يتطلب الأمر من جهة القاضي تقدير وتمحيص أقوال الشاهد حتى يمكن التحقق من مدى صحة أقواله وهو جدير بذلك لما له من ملكتي النقد والتفسير أما إذا كان مصدر هذه الشهادة القاضي نفسه فمن الصعب عليه القيام بالرقابة المطلوبة إذ يقع وقتها في صراع مع نفسه لأن الأمر يستلزم أن تكون المعلومات التي يدلي بها بعيدا عن التأثيرات الشخصية والتحيز[226].

(224) أحمد. هلالي عبد اللاه (2011). *النظرية العامة للإثبات الجنائي*. ص 476.
(225) عثمان. حازم محمد حنفي (2016). *الدليل الإلكتروني ودوره في المجال الجنائي*. ص261.
(226) حسني. محمود نجيب (2016). *شرح قانون الإجراءات الجنائية*. مصر: دار النهضة العربية. ص793.

2– عدم جواز أن يحكم القاضي بناءً على رأي الغير:

أما فكرة أنه لا يجوز أن يقضي القاضي في جريمة نشر الأخبار الكاذبة عبر وسائل التواصل الاجتماعي بناء على رأي الغير فهى مما يتقيد به القاضي الجزائي أيضا في تكوين اقتناعه عدم التعويل على رأي الغير، بل يلزم أن يكون هذا الاقتناع من مصادر يستقيها بنفسه من التحقيق في الدعوى وهي إحدى النتائج المهمة المترتبة على قاعدة وجوب مناقشة الدليل في المواد الجنائية يستوى في ذلك أن يكون دليلا تقليديا أم دليلا رقميا، وإعمالًا لذلك لا يجوز أن يحيل الحكم في شأن وقائع الدعوى ومستنداتها إلى دعوى غير مطروحة أو أن تستند المحكمة إلى وقائع وأدلة تستقيها من أوراق قضية أخري لم تكن مضمومة للدعوى التي تنظرها للفصل فيها ولم تكن مطروحة على بساط البحث بالجلسة تحت نظر الخصوم[227].

لكنه يلاحظ أنه وان كان من الواجب أن يصدر الحكم بناء على عقيدة للقاضي يستقيها هو مما يجريه من التحقيقات مستقلًا في تكوين هذه العقيدة بنفسه لا يشاركه غيره فيها الا أن ذلك لا يعنى منع القاضي بصفة عامة من الأخذ برأي الخبير متى اقتنع به هو؛ حيث يجب عليه أن يبين في هذه الحالة أسباب اقتناعه بهذا الرأي باعتباره من الأدلة المقدمة إليه في الدعوى المطلوب منه أن يفصل فيها.

(227) حسني. محمود نجيب (2016). *شرح قانون الإجراءات الجنائية*. ص 794.

المبحث الثاني: إشكاليات مكافحة جريمة نشر الأخبار الكاذبة عبر وسائل التواصل الاجتماعي

للتعرف على إشكاليات مكافحة تلك الجريمة، سيتم تقسيم هذا المبحث إلى مطالب ثلاثة، كالآتي:

المطلب الأول: خصائص الدليل الرقمي وصعوبة الحصول عليه

من خلال التعريفات العديدة السابقة في الدليل الرقمي يتضح لنا أن الدليل الرقمي يتميز بعدد من الخصائص، تتمثل فيما يلي:

عدم وجود أثر مادي في جريمة نشر الأخبار الكاذبة عبر وسائل التواصل الاجتماعي:

تواجه سلطة الاستدلال أو التحقيق الجنائي المحاكمة صعوبة في كشف وتحصيل الأثر المادي في جريمة نشر الأخبار الكاذبة عبر وسائل التواصل الاجتماعي لأنها لا تترك أثرًا خارجيًا [228]؛ لأن جرائم الشائعات المعلوماتية لا عنف فيها، ولا سفك دماء، لأنها لا تترك في الغالب أية آثار مادية كتلك التي تخلفها الجرائم التقليدية، حيث إنها لا تخلف لا سكينًا ولا سلاحًا ولا ظروفًا فارغة لطلقات نارية ولا بقعًا دموية أو غير ذلك من الآثار المادية [229]. إنما هي عبارة عن نبضات إلكترونية غير مرئية بالعين المجردة، فهي تصل في حجمها وشكلها ومكان تواجدها إلى درجة شبه منعدمة بحيث إنه لا يمكن رؤيتها إلا من خلال الاستعانة بأجهزة ووسائل تقنية تظهرها للعيان [230]؛ حيث إنها أرقام وبيانات تتغير أو تمحى من السجلات، أو يتم نقلها المعلومات دون وجود أي أثر خارجي مرئي، فهي جريمة فنية [231]. وقد يترك الجاني أثرًا يدل على الصلة على وقوع جريمة نشر الأخبار الكاذبة عبر وسائل التواصل الاجتماعي فلا تُفصح شخصه، لصعوبة التتبع والفحص للكم الهائل من البيانات والمعلومات المدرجة بالأنظمة

(228) أبو القاسم. طاهر محمود (2019). *الجرائم المعلوماتية* "صعوبات وسائل التحقيق فيها وكيفية مواجهتها". الإمارات العربية المتحدة: منشورات جامعة الدول العربية. ص127.

(229) مصطفى. عائشة بن قاره (2010). حجية الدليل الإلكتروني في مجال الإثبات. مصر: دار الجامعة الجديدة، ص62.

(230) الغفلي. محمد خليفة (2021). ***حجية الدليل الرقمي في الإثبات الجنائي دراسة مقارنة***. (رسالة دكتوراه). مصر: جامعة عين شمس. ص54.

(231) عوض. محمد محي الدين (1993م) "مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات". ورقة عمل. ***للمؤتمر السادس للجمعية المصرية للقانون الجنائي في مجال الأضرار بالبيئة***. الجرائم الواقعة في مجال تكنولوجيا المعلومات. أعمال المؤتمر. مصر: دار النهضة العربية. ص 368.

التكنولوجيا، مع تنامي السعة التخزينية للوسائل الممغنطة والضوئية وما تحتويه من كميات ضخمة من البيانات والمعلومات وهي إحدى الصعوبات التي تواجه المحققين بتتبع الآثار الإلكترونية إضافة إلى أن الكثير من الجناة يعمدوا إلى إخفاء هويتهم فيحبط محاولة المحققين بكشفهم والتعرف عليهم.

1. **سهولة محو الأدلة في زمن قصير:**

إن الدليل المتحصل من الوسائل الإلكترونية هي نبضات ونقاط إلكترونية ليست مرئية تتدفق عبر النظام الإلكتروني، مما يجعل أمر محو الدليل كليًا أو طمسه من قبل الفاعل أمرًا سهلًا[232]. إذ يقوم مرتكبو جريمة نشر الأخبار الكاذبة عبر وسائل التواصل الاجتماعي بالتلاعب في النبضات والذبذبات الإلكترونية التي تسجل عن طريقها المعلومات والبيانات لإخفاء ما قاموا به من تسلل إلى قواعد البيانات والمعلومات وما أجروه من تعاملات مع شبكات الإنترنت مستغلين ضعف الأنظمة الرقابية فيدخلون إلى شبكات الإنترنت أو إخفاء برامج خاصة ضمن برنامجه فلا يشعر بها القائمون بالتشغيل. كما قد يتعمد الجاني محو الدليل بعد إدخال التعديلات التي يريدها على البيانات والمعلومات بإرجاع الوضع إلى ما كان عليه قبل التعديل بعد اطلاعه عليها ونسخها ولا يمكن كشف ذلك بالطرق التقليدية إنما لابد من استخدام إجراءات جنائية ذات طبيعة فنية[233] خصوصًا أن إجراءات جمع الأدلة لم ترد في القانون على سبيل الحصر، ولذلك يجوز للمحقق أن يباشر أي إجراء آخر يرى فيه ميزة للإثبات وحيث إنه لا يترتب على اتخاذه تقييد لحريات الأفراد أو مساس بحرمة مساكنهم[234].

(232) المومني. نهلا عبد القادر (2008). *الجرائم المعلوماتية*. الأردن: دار الثقافة للنشر والتوزيع. الطبعة الأولى. ص56.
(233) حجازي. عبد الفتاح بيومي (2007م). *مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت*. مصر: دار الكتب القانونية. ص 58.
(234) إبراهيم. خالد ممدوح (2007م). *التقاضي الالكتروني*. مصر. الطبعة الأولى ص323.

2. **نقص الخبرة:**

تقوم الجريمة على تخصصات عديدة علمية وفنية وتقنية في غاية من الدقة والتطور السريع بدرجة يصعب على رجال البحث والتحقيق التعامل مع كافة صورها وأنماطها بمعلوماتهم العادية وتدريباتهم الأولي على تقنيات أجهزة الحاسب والإنترنت لنقص الخبرة والكفاءة لدى القائمين بالبحث والتحقيق في هذه الجرائم؛ فيكون من العبث توقع كشفهم لهذه الفئة من الجرائم والوصول إلى القرائن والدلائل المستحقة في مجال إثباتها، وكيفية معاينتها والتحفظ عليها وفحصها فنيًا، لذلك يلزم تدريب رجال الضبط والمحققين والقضاة على معالجة هذا النوع من القضايا لتمكينهم من الفصل فيها.

3. **عدم الإبلاغ عن الجريمة:**

يتجه بعض شراح القانون الجزائي إلى أن غالبية الجرائم المعلوماتية تكتشف مصادفة وليس بطريق الإبلاغ عنها [(235)]؛ بل ويعد وقتًا طويلًا من ارتكابها فلا يعرف عدد هذه الجرائم الحقيقي لإخفاء معالم الجريمة وصعوبة تتبع مرتكبيها. حيث يستخدم الجناة تشفير وترميز البيانات المخزنة إلكترونيًا أو المنقولة عبر وسائل التواصل الاجتماعي لإعاقة الوصول إلى الأدلة التي تدين المتهم إما لعدم اكتشاف الضحية لها وإما لخشيته من التشهير مما يدفع المجني عليه في جريمة نشر الأخبار الكاذبة عبر وسائل التواصل الاجتماعي إلى عدم التعاون مع جهات التحقيق خوفًا مما يترتب عليه من دعاية ضارة وضياع ثقة المساهمين خصوصًا إذا كان من وقعت عليه شخصية مشهورة أو مؤسسة مالية أو مشروع صناعي ضخم أو شخص ضعيف لا حيلة له في الرد، فيصعب على أجهزة الرقابة على البيانات المخزنة كشف التلاعب في الوصول غير المشروع إلى البيانات والمعلومات المخزنة، وتعوق عمل جهات التحقيق في

(235) حجازي. عبد الفتاح بيومي (2007م). *الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت*. ص24.

Taking note of resolution 9, on computer-related crimes, adopted by the Eighth United Nations Congress on the Prevention of crime and the treatment of offenders, in which states were called upon to intensify their efforts to more effectively combat computer-related abuses.

الموقع على الشبكة الدولية. التصفح في: 2021/6/1:

http://context.reverso.net/translation/arabic-english.

البحث عن الأدلة التي تدين المتهم وضبطها لأنها محاطة بسياج من التقنية الفنية تحول دون كشفها وضبطها، أو أن الجريمة مرتكبة بقدرة عالية من الخبرة.

4. صعوبات تتعلق بالاختصاص:

تعد جريمة نشر الأخبار الكاذبة عبر وسائل التواصل الاجتماعي من الجرائم العابرة للحدود بسبب الترابط بين شبكات المعلومات المحلية والإقليمية والدولية بشكل تلاشت معه الحواجز الجغرافية والمسافات، إذ يستطيع المجرم الإلكتروني إخفاء هويته، ونقل المواد المكونة للشائعة من خلال أدوات ووسائل موجودة في دول مختلفة، في قارات مختلفة قبل الوصول إلى المرسل إليهم، نتيجة القدرة على التنقل إلكترونيًا من شبكة إلى أخرى والنفاذ إلى قواعد البيانات في قارات مختلفة، بحيث تقع الجريمة في عدة دول وتحكمها عدة قوانين وقواعد معينة بذلك، مما يشكل تحديًا أمام الجهات القضائية في تطبيق القانون ويزيد من صعوبة التحقيق فيها، وهنا تنشأ مشكلة تنازع الاختصاص التشريعي والقضائي بين الدول التي تأثرت بالجريمة المرتكبة. وتثار أيضًا مشكلة التحقيق خارج إقليم الدولة للبحث عن أدلة الجريمة، خاصة في ظل اختلاف تشريعات الدول في القواعد الموضوعية والإجرائية في جريمة نشر الأخبار الكاذبة عبر وسائل التواصل الاجتماعي مما يجعل مهمة جهات البحث والتحقيق في هذه الجرائم مهمة صعبة وشاقة.

5. صعوبة وجود تعاون دولي:

إن غياب التعاون والتنسيق بين الأفراد والشركات والدول يؤدي دورًا رئيسًا ومؤثرًا في مد جريمة نشر الأخبار الكاذبة عبر وسائل التواصل الاجتماعي عبر الدول وتتعدى حدود الإقليم وانحسار أساليب المكافحة ومن ثم صعوبة إثباتها [236]، يقابله في ذات الوقت تعاون واضح بين محترفي الإجرام المعلوماتي،

(236) عبد العظيم. عمر أبو الفتوح (2010م). *الحماية الجنائية للمعلومات المسجلة إلكترونيًا*. مصر: دار النهضة العربية. ص438.

إضافة إلى البرامج التي يستعين ها القراصنة في أنشطتهم الإجرامية؛ فإنهم يتعاونون فيما بينهم ويتبادلون النصائح والخبرات فيما يتعلق بأنشطتهم مما يزيد من فاعلية وخطورة هجومهم وخصوصًا في ظل قصور وعدم فاعلية سياسة الدفاع الخاصة والمنفردة ضد الجريمة المعلوماتية. (237)

ويرى الباحث أن المشكلة التي تثيرها جريمة نشر الأخبار الكاذبة عبر وسائل التواصل الاجتماعي تتعلق بإثبات الجرائم الواقعة عليها، فالضبط المترتب على التفتيش لا يمكن وقوعه إلا إذا تبين أن هناك جريمة ارتكبت بالفعل، ولذلك فإن الجرائم الواقعة على الكيانات المادية يسهل اكتشاف أمرها وضبطها، وأما الجرائم التي تقع على الكيانات المعنوية فإنه يصعب اكتشافها إذا ظلت على صورتها المعنوية في شكل نبضات أو ذبذبات، وأما إذا تحولت هذه الكيانات إلى مستخرجات أو مستندات أو سجلات فإنه يسهل الوصول إلى الجرائم التي تُرتكب عليها. وبتطبيق ذلك على جريمة نشر الأخبار الكاذبة عبر وسائل التواصل الاجتماعي، فإنه لا يمكن العقاب عليها إلا بوقوع السلوك المادي الذي به تقوم الجريمة.

(237) منصور. حاتم عبد الرحمن (2002). *الإجرام المعلوماتي*. مصر: دار النهضة العربية. الطبعة الأولى. ص153.

المطلب الثاني: جريمة نشر الأخبار الكاذبة ومشكلة قبول الدليل الرّقمي

القاعدة التي تسود التشريعات الجزائية في الإثبات أن المحكمة تحكم في الدعوى بناء على اقتناعها الذي تكون لديها من الأدلة المقدمة في أي دور من أدوار التحقيق أو المحاكمة، ولا سلطان عليها في ذلك إلا ضمير القضاة ولا تطالب إلا ببيان سبب اقتناعها بدليل دون آخر فهي لا تلزم بإقرار صادر من المتهم أو شهادة إثبات أسندت الجريمة أليه أو شهادة دفاع نفت التهمة عنه أو رأي قدمه خبير إلا إذا اقتنعت له(238).

كما أن الأدلة الجزائية التي تستقي منها المحاكم قناعتها ليست محددة حصرا لكن القانون ذكر بعضها وهي الغالب الشائع وتتمثل في الإقرار والمحاضر وشهادة الشهود ومحاضر التحقيق والكشوف الرسمية الأخرى وتقارير الفنيين والخبراء، ثم جاء القانون بنص عام ليشمل غيرها من الأدلة بقوله: "والقرائن والأدلة الأخرى المقررة قانونا" وعلى ذلك فإنه يكون للقاضي كامل الحرية في تقدير كافة الأدلة المطروحة عليه في الدعوى وله أن يفاضل بين جميع هذه الأدلة فيأخذ بما يطمئن إليه من أدلة ويعرض عما لا يطمئن إليه من أدلة أخرى.

وقد أقر المشرع للدليل الرقمي ذات الحجية المقررة للدليل التقليدي، وبذلك يمكن اعتبار الأدلة الرقمية هي أدلة مقبولة إذا توافرت فيها شروط معينة وللقاضي الجنائي الحرية في تقدير جميع أدلة الدعوى الجزائية بغض النظر عن مصدرها الذي استمدت منه طالما كان مشروعا ويستوي في ذلك الدليل الجنائي التقليدي والدليل الجنائي الرقمي فباب الإثبات مفتوح على مصراعيه أمامه يأخذ بأي دليل يطمئن إليه وجدانه ويطرح كل دليل يدور الشك حوله وذلك بغية الوصول إلى الحقيقة (239).

تتميز المستندات الإلكترونية بطابع خاص تنفرد به فيما يتعلق بقوتها الثبوتية أمام المحكمة سواء فيما يتعلق بإثبات أركان الجريمة أو بإثبات الشرط المفترض فيها.

---

(238) عبد اللطيف. براء منذر (2009). *شرح قانون أصول المحاكمات الجنائية*. الأردن: دار الحامد للنشر والتوزيع. ط1. ص216.

(239) يوسف. أمير فرج. (2016). *الإثبات الجنائي للجريمة الإلكترونية والاختصاص القضائي بها "دراسة مقارنة للتشريعات العربية والأجنبية"*. مصر. مكتبة الوفاء القانونية. ص365.

ولما كان القاضي الجنائي يتمتع بحرية في تكوين عقيدته، فإنه ليس هناك ما يمنع من أن يستند في تكوين ذلك الاقتناع على مخرجات الحاسب الآلي. بيد أن تلك المخرجات سواء كانت بيانات مسجلة في داخل الجهاز أو على ديسك أو شريط ممغنط أو على مخرجات ورقية يصح اعتبارها قرينة تضاف إلى قرائن أخرى لكي تكون اقتناع القاضي الجنائي، ذلك أن تلك المخرجات يمكن التلاعب فيها وليست من القوة بحيث يصح اعتبارها دليلًا واحدًا يسند الحكم الصادر بالإدانة. ويطرح ذلك مسألة القوة الثبوتية لمخرجات الحاسب الآلي أمام القاضي الجنائي، أما أمام القاضي المدني، فإن تلك المخرجات تتعارض مع المحررات التقليدية، ومن ثم فإنه يصعب الاستناد إليها، إلا إذا صدر قانون ينظم تلك المسألة في الموضوعات المدنية.

وإذا كانت القوة الثبوتية للمستندات الإلكترونية أمام القاضي الجزائي في التشريعات اللاتينية يعتريها أوجه من الضعف، فإن تلك المستندات كانت مجردة أصلًا من القوة الثبوتية أمام القاضي الجنائي في التشريعات الأنجلو – أمريكية بسبب أن تلك التشريعات تعتنق نظام الإثبات المقيد، ولم تكن مخرجات الحاسب الآلي قد نظمها القانون في تلك التشريعات. هذه الطائفة من التشريعات لم تكن تقبل مخرجات الحاسب الآلي أمام القاضي الجنائي إلا إذا كانت مشفوعة بشهادة صاحب الجهاز أو مدير النظام أو المسئول عنها [240].

فالإثبات الجنائي إجراء موجه مباشرةً بهدف الوصول إلى اليقين القضائي طبقًا لمعيار الحقيقة الواقعية، وذلك بشأن الاتهام أو أي تأكيد أو نفي آخر يتوقف عليه إجراء قضائي، بمعنى آخر هو إقامة الدليل على وقوع الجريمة ونسبتها إلى فاعل معين [241].

(240) الغفلي. محمد خليفة (2021). *حجية الدليل الرقمي في الإثبات الجنائي*. ص376.
(241) المصدر نفسه. ص377.

وبالرجوع إلى النظم السائدة في معظم التشريعات المقارنة، نجد أنها تعتمد نظام الأدلة المعنوية، وهو يقوم على مبدأ الاقتناع الشخصي للقاضي الجنائي، وبمقتضاه يتمتع القاضي بحرية واسعة في تقدير الأدلة، حيث يوفر له استقلالًا تامًا لتكوين قناعته القضائية حول قيمة الأدلة المعروضة أمامه [242].

سلطة القاضي الجنائي في قبول دليل الإثبات:

تُعد حرية القاضي في تقدير الأدلة المعروضة عليه في الدعوى نتيجة طبيعية لمبدأ الاقتناع الشخصي، فهو غير ملزم بإصدار حكم بالإدانة أو بالبراءة لتوافر دليل معين مادام أنه لم يقتنع به [243].

فنظرًا للرغبة في حماية الحرية الفردية، أصبح كل دليل يؤدي إلى اليقين هو دليل إثبات، فلا يملك القاضي استبعاد أي دليل منها، بدعوى أنه غير مقبول في الإثبات [244]، وبذلك يختلف الإثبات الجنائي عن الإثبات المدني، فأدلة الإثبات حرة في المسائل الجنائية، بينما هي مقيدة في المسائل المدنية، وإن كان قانون أصول المحاكمات الجنائية لا يتضمن سوى بعض النصوص في البينات، إلا أن الإثبات في المسائل المدنية نظمه قانون منفصل بذاته، بشأن البينات في المواد المدنية والتجارية [245].

كما أن دور القاضي الجنائي ليس دورًا سلبيًا مثل دور القاضي المدني الذي يقتصر دوره على الموازنة بين الأدلة التي يقدمها أطراف الدعوى، ثم يرجح أيها أغلب، بل إن دوره إيجابي، فمن سلطته بل واجب عليه تحرى الحقيقة، وذلك بجميع الطرق، ثم يكون قناعته بمنتهى الحرية [246].

---

(242) أبو عيد. إلياس. (2005). *نظرة الإثبات في أصول المحاكمات المدنية والجنائية "بين النص والاجتهاد والفقه"*: دراسة مقارنة، لبنان: منشورات زين الحقوقية. ص203.

(243) بلال. أحمد عوض. (2015). *قاعدة استبعاد الأدلة المتحصلة بطرق غير مشروعة في الإجراءات الجنائية المقارنة*. مصر: دار النهضة العربية. ص84.

(244) المرصفاوي. حسن صادق. (2012). *قانون الإجراءات الجنائية مع تطوراته وأحكام النقض في مائة عام*، مصر: منشأة المعارف، ص217.

(245) المادة (15) من القانون التجاري الجزائري تنص على أنه: "لا يجوز الأمر بتقديم الدفاتر وقوائم الجر، إلى القضاء إلا في قضايا الإرث، وقسمة الشركة، وفي حال الإفلاس".

(246) هرجه. مصطفى مجدي (2009). *الإثبات في المواد الجنائية في ضوء أحكام محكمة النقض*. مصر: دار المطبوعات الجامعية. ص54.

الاقتناع الشخصي للقاضي الجنائي:

تنصر حرية الإثبات في المسائل الجنائية للقاضي وللخصوم في الدعوى، فللقاضي الحرية الكاملة في استقصاء أدلة الإثبات وهو في ذلك غير مقيد بنوع معين منها ومرجعيته هنا لاقتناعه الشخصي. والذي يمكن تعريفه بأنه: "التقدير الحر المسبب لعناصر الإثبات في الدعوى، فهو البديل عن نظام الأدلة القانونية"[247].

فالاقتناع هو حالة ذهنية تمتاز بكونها ذات خاصية لتفاعل ضمير القاضي عند تقديره للأمور، فالاقتناع يعبر عن ذاتية وشخصية القاضي [248]، وهذا المبدأ يتجلى في شقين: الأول حرية القاضي الجنائي في أن تكون قناعته من أي دليل يطمئن إليه، دون التقيد في تكوين هذه القناعة بدليل، والثاني حرية القاضي الجنائي في تقدير الأدلة المعروضة عليه [249].

على أن حرية التقدير هذه، يجب ألا تصل إلى حدود التحكم الكامل [250]، فيجب أن يخضع اقتناع القاضي دائمًا للعقل والمنطق، باعتباره عملاً ذهنيًا أو عقليًا يحصله القاضي في صمت وخشوع في مناخ من الصدق وسلامة الطوية.

وبناءً عليه، فإن حرية القاضي في التثبت تختلف تمامًا عن التحكم، فالتثبت الحر يعني أن القاضي له الحرية في تقييم أدلة الإثبات دون قيد سوى مراعاة واجبه القضائي.

ومما سبق ذكره، يتضح لنا أن الاقتناع الشخصي للقاضي الجنائي يتميز بخاصيتين تخلعان عنه صفة الوضوح والتحديد، وهما: خاصية الذاتية، وخاصية النسبية.

(247) الجوهري. كمال عبد الواحد. (1999). تأسيس الاقتناع القضائي والمحكمة الجنائية العادلة. مصر: دار محمود للنشر. ص14.
(248) الربيش. عبد الله بن صالح بن رشيد. (1424). ***سلطة القاضي الجنائي في تقدير أدلة الإثبات بين الشريعة والقانون وتطبيقاتها في المملكة العربية السعودية***. (رسالة ماجستير). السعودية. جامعة نايف العربية للعلوم الأمنية. ص 75.
(249) سرور. أحمد فتحي. (2016). *الوسيط في قانون الإجراءات الجنائية*. مصر: دار النهضة العربية. الطبعة 12. ص774.
(250) المصدر نفسه. ص 774.

تكوين يقين القاضي الجنائي:

إن هدف النشاط الذهني الذى يكون قناعة القاضي والذي يقع على الدليل موضع التقدير تكون بهدف الوصول إلى الحقيقة، ويقصد بالحقيقة هنا الحقيقة القضائية، التي قد لا تكون –الحقيقة القضائية– هي ذاتها الحقيقة الواقعية، حيث إنه من الصعب الحصول على اليقين التام في مسألة إثبات الوقائع المادية بصفة عامة، والأفعال الجنائية على وجه الخصوص [251]، ويعود هذا إلى سببين: أولهما أنه لا يوجد أي دليل يمكن أن نصل بواسطته إلى اليقين التام – اليقين المادي للحقيقة– الذي لا يوجد خارج إطار علم الرياضيات، وثانيهما تميز اليقين القضائي بصفة الذاتية، حيث إنه ناتج عن عمل ذهني أو عقلي مما قد يعرض اقتناعه إلى الاختلاف والتنوع في التقدير بين قاضٍ وآخر[252].

مبدأ حرية القناعة الوجدانية للقاضي الجنائي:

لقد تركت كل مرحلة من مراحل تطور المجتمع بصمتها المميزة على جبين الإثبات الجنائي، وصبغته بصبغة خاصة، تعكس الأحوال السياسية والاقتصادية والاجتماعية والدينية والتاريخية السائدة فيه [253].

وقد أخذ قانون الإجراءات الجزائية الإماراتي بمبدأ حرية تكوين اقتناع القاضي الجنائي، حيث إن المادة (209) من القانون تنص على أنه: "يحكم القاضي حسب القناعة التي تكونت لديه ومع ذلك لايجوز له أن يبنى حكمه على أي دليل لم يطرح على الخصوم في الجلسة"، ويتضح من النص السابق أن القاضي الجنائي له سلطة تقديرية واسعة في تكوين قناعته من الدليل الذي يطمئن إليه، ويحكم بالإدانة

(251) نصر الدين. مروك. (2007). *محاضرات في الإثبات الجنائي، النظرية العامة للإثبات الجنائي*. الجزائر: دار هومة للطباعة والنشر والتوزيع. الجزء الأول. ص629.

(252) أحمد، هلالي عبد اللاه (2011). *النظرية العامة للإثبات في المواد الجنائية*. ص 406.

(253) المصدر نفسه. ص31.

أو بالبراءة طبقًا لما يمليه عليه ضميره واقتناعه [254]. ولا يلتزم القاضي الجنائي بما هو مكتوب في التحقيق الابتدائي أو في محاضر الاستدلالات، إلا إذا كان في القانون نص على خلاف ذلك [255].

وقد أخذت المحكمة الاتحادية العليا في أحكامها [256] بحرية القاضي الجنائي في تكوين قناعته مؤكدة على تمتعه بسلطة واسعة في جمع الأدلة وتقديرها في نطاق الجرائم التعزيرية، فلا يستخدم ترتيبًا معينًا في الأخذ بها، وله أن يستند إلى دليل ويطرح الأدلة الأخرى، ففهم الوقائع في الدعوى وتقييم أدلتها وترجيح ما تراه المحكمة راجحًا وجديرًا بالاعتبار واستخلاص الحقيقة منها يدخل في اختصاص محكمة الموضوع دون رقابة عليها [257]. ورغم ذلك فإن حرية المحكمة في تكوين قناعتها مشروطة بأن تبنى المحكمة قناعتها على أسباب سائغة لها أصلها من الأوراق، وتوصل إلى النتيجة التي انتهى الحكم إليها بما ينبئ أنها محصت الدعوى وأحاطت بظروفها، وبكافة الأدلة المقدمة فيها [258].

القيود الواردة على حرية القاضي الجنائي في قبول دليل الإثبات:

إن أسمى غرض تنشده التشريعات الإجرائية الجنائية هو إصابة القاضي الحق في حكمه [259]، ولايوجد الحق بمعزل عن دليله عند المنازعة فيه، فدليل الإثبات هو عماد حياة الحق، أي ليس من المتصور قيام دعوى قضائية دون أن تثور فيها مسألة الإثبات القضائي، والذي يعني تقديم الدليل أمام القضاء بالطرق التي حددها القانون لإثبات المصدر المنشئ للحق [260].

---

(254) سلامة. مأمون (2015). *الإجراءات الجنائية في التشريع المصري*. مصر: دار النهضة العربية. ص83.

(255) عبد الستار. فوزية. (2018). *شرح قانون الإجراءات الجنائية*. مصر: دار النهضة العربية. ص456.

(256) المحكمة الاتحادية الإماراتية العليا، نقض جزائي، جلسة 194/6/25، الطعن رقم 19 لسنة 6 ق. ع، جزائي، جلسة 1994/3/23.

(257) المحكمة الاتحادية الإماراتية العليا، نقض جزائي، جلسة 1993/3/6، الطعن رقم 162 لسنة 1991م، ق. ع. شرعي.

(258) المحكمة الاتحادي الإماراتية العليا، نقض جزائي، جلسة 1993/11/10، الطعن رقم 90 لسنة 19 ق. ع. جزائي.

(259) الربيش. عبد الله بن صالح بن رشيد. *سلطة القاضي الجنائي في تقدير أدلة الإثبات بين الشريعة والقانون* وتطبيقاتها في المملكة العربية السعودية. ص 146.

(260) عبيد. رؤوف. (1986). *ضوابط تسبيب الأحكام الجنائية وأوامر التصرف في التحقيق*. مصر: دار الجيل للطباعة. ص500.

وهناك عدة مذاهب أساسية تحكم إمكانية اقتناع القاضي الجنائي بدليل الإثبات هي [261]:

مذهب الإثبات الحر أو المطلق، ومذهب الإثبات القانوني أو القيد، ومذهب الإثبات المختلط.

وقد أخذ المشرع الإماراتي في تنظيم الإثبات بالمذهب المختلط بحيث لم يجعل دور القاضي سلبيًا بحتًا بل خوله سلطات في تقدير الأدلة واستكمالها، لتمكينه من الوصول إلى الحقيقة فللقاضي أن يوجه اليمين المتممة من تلقاء نفسه والانتقال لمعاينة المتنازع فيه وانتداب خبير عند الاقتضاء [262].

الشروط الواجب توافرها في الأدلة الثبوتية الرقمية لكي تكون مقبولة:

إذا كان الأصل هو حرية القاضي الجنائي في أن يستقي قناعته من أي دليل يطمئن إليه، إلا أنه توجد بعض الضوابط على هذا الأصل يجب على القاضي الالتزام بها [263]، على النحو الآتي:

الشرط الأول: الحصول على الدليل الرقمي بصورة مشروعة:

رغم أن قاعدة شرعية الجرائم والعقوبات تعد إحدى الركائز الرئيسية للتشريعات الجنائية الحديثة، إلا أنها لا تكفي بمفردها للحفاظ على حرية الإنسان، لذلك كان من الواجب تدعيم هذه القاعدة بقاعدة ثانية تحكم تنظيم الإجراءات التي تتخذ قبل المتهم على نحو يكفل احترام الحقوق والحريات الفردية، وهذه القاعدة تُسمى بالشرعية الإجرائية أو قاعدة مشروعية الدليل الجنائي، ويقصد بها ضرورة توافق الإجراءات التي أدت للحصول على الدليل، مع القواعد القانونية والأنظمة المستقرة في ضمير وجدان المجتمع المتمدن [264].

---

(261) ناجي. صالح يحيي رزق. (2008). ***سلطة القاضي الجنائي في تقدير أدلة الإثبات الحديثة***. "دراسة مقارنة". (رسالة ماجستير). مصر: معهد البحوث والدراسات العربية. ص56.

(262) القاضي. ماهر سلامة العوفي (2015). *أحكام جرائم التزوير التقليدي والإلكتروني*: دراسة تأصيلية لجرائم التزوير في قانون العقوبات والقوانين الخاصة والتزوير الإلكتروني في دولة الإمارات العربية المتحدة. معهد دبي القضائي. ص103.

(263) سويدان. مفيدة (1985). ***نظرية الاقتناع الذاتي للقاضي الجنائي***. (رسالة دكتوراه). مصر: جامعة القاهرة. ص44.

(264) أحمد. هلالي عبد اللاه (2011). *النظرية العامة للإثبات الجنائي*. ص497.

وعليه، لا يصير الدليل مشروعًا ومقبولًا في عملية الإثبات والتي يتم من خلالها إخضاعه للتقدير إلا إذا تمت عملية البحث عنه أو الحصول عليه، وعملية تقديمه إلى القضاء بالطرق التي حددها القانون[265].

حيث إن الخصومة الجنائية تقوم على كفالة حرية المتهم، إضافة إلى إثبات سلطة الدولة في توقيع العقاب[266]، ومن ثم فإنه يجب على القاضي أن يثبت توافر هذه السلطة تجاه المتهم من خلال إجراءات مشروعة يتم فيها احترام الحريات وتؤمن الضمانات التي حددها القانون[267]، أما إذا جهل أو تجاهل قاعدة قانونية فإن هذا ينعكس على الاقتناع الذي كونه لأنه نتيجة الخطوات التي اتخذها، وهو نتيجة العمليات التي أجراها بطريقة يشوبها الخطأ أو الفساد[268]، ومؤدي هذا أن هذه السمة تتصل اتصالا وثيقًا بالمنهج القضائي في الاقتناع أو بكيفية تحديد ملامحه[269].

ولقد تناولت الاتفاقية الخاصة بحماية الأشخاص في مواجهة مخاطر المعالجة الآلية للبيانات ذات الطبيعة الشخصية التي صادقت عليها لجنة الوزراء التابعة للمجلس الأوروبي في 1981/1/28م ضرورة أن البيانات المضبوطة تكون صحيحة ودقيقة وكاملة، وممتدة بطرق مشروعة، وأن تكون مدة حفظها محددة زمنيًا، ولا يجوز إفشاؤها أو استخدامها في غير الأهداف المخصصة لها، وحق كل شخص في التعرف والاطلاع على البيانات المسجلة المتعلقة به وتصحيحها وتعديلها ومناقضتها وإزالتها إذا كانت باطلة. أما إذا كانت بيانات الحاسب الآلي الموجودة في ملفات الشرطة غير قانونية، فذلك يلزم بضرورة محو هذه البيانات، ولا يمكن استعمالها كدليل جنائي طبقًا لمبدأ استبعاد الأدلة غير القانونية والحفاظ على سرية البيانات التي يتم الحصول عليها بطريقة مشروعة احترامًا للحق في الخصوصية. فيجب التقيد

(265) أحمد. هلالي عبد اللاه (2011). النظرية العامة للإثبات الجنائي. ص 798.
(266) الغافري. حسين بن سعيد. سلطة القاضي الجنائي في قبول الأدلة المستخرجة من الإنترنت. مقال منشور على شبكة الإنترنت تاريخ الدخول 2021/7/1، في: www.omanlegal.net
(267) سرور. أحمد فتحي. *الوسيط في قانون الإجراءات الجنائية*. ص751.
(268) منصور. محمد حسين (2009). *قانون الإثبات. مبادئ الإثبات وطرقه*. مصر: دار الجامعة الجديدة للنشر. ص9.
(269) الجوهري. كمال عبد الواحد. *تأسيس الاقتناع القضائي والمحاكمة الجنائية العادلة*. ص 32.

بقاعدتين هما: الأولى: قاعدة: "الأصل في الأشياء الإباحة – في المعاملات – حتى يرد نص"هي قاعدة موضوعية تحكم شرعية التجريم والجزاء الجنائي فكان من الواجب صدور قانون ينظم الإثبات الجنائي، ويُدخل فيها الأدلة العلمية ومنها الدليل الإلكتروني كالدول التي أخذت بقانون الإثبات الجنائي مثل بريطانيا. والثانية: قاعدة: "الأصل في الإنسان البراءة حتى يصدر حكم جنائي بات" هي قاعدة شرعية إجرائية تحكم كل مراحل الدعوى الجنائية. بأن كل الأدلة يجب أن يتم الحصول عليها دون انتهاك حق أساسي للمتهم حتى لا يحكم ببطلانه. ولذلك يجب أن تكون المخرجات الإلكترونية أو الأدلة الناجمة عن الحاسب الآلي سليمة ومشروعة حتى يمكن الحكم بالإدانة (270)، ولقاعدة البينة على من ادعى وجهان لعملة واحدة. ومن ثم يترتب على هاتين القاعدتين ما يلي:

1. ضرورة احترام النصوص في تحصيل الدليل: يجب أن يتفق الإجراء الذي نتج عنه الدليل الناتج عن الحاسب الآلي مع القواعد والأنظمة القانونية الثابتة عند المجتمع. ويتعين على القاضي الجنائي أن يثبت الحق في العقاب للمتهم من خلال إجراءات مشروعة تحترم فيها الحريات وتؤمن فيها الضمانات التي حددها القانون سواء كانت الأدلة تقليدية أو كانت ناتجة عن الحاسب الآلي.
2. احترام حقوق الإنسان عند تحصيل الدليل الإلكتروني: لا تقتصر مشروعية الدليل على مجرد التطابق مع القاعدة القانونية التي ينص عليها المشرع فقط بل يجب أيضًا مراعاة إعانات حقوق الإنسان والمواثيق والاتفاقات الدولية وقواعد النظام العام وحسن الآداب السائدة في المجتمع وما تقرره الدساتير الحديثة التي تنظم القواعد الأساسية في الاستجواب والتوقيف والحبس والتفتيش وغيرها، بحيث يتقيد المشرع بها مما يقتضي رفض اللجوء للوسائل التي "تجرد الإنسان من قدراته الذهنية" لأنها نوع من "التعسف" كالعقاقير المخدرة أو ما يسمى مصل الحقيقة، وجهاز كشف الكذب، ... الخ فإقرار مبدأ حرية الإثبات الذي يمكن الاعتماد عليه من كل طرف من أطراف

(270) الجوهري. كمال عبد الواحد. تأسيس الاقتناع القضائي والمحاكمة الجنائية العادلة. ص34.

الدعوى الجنائية بما في ذلك المتهم والنيابة العامة والقاضي ولا يعني مبدأ القناعة الوجدانية للقاضي الجنائي أن يحكم وفق هواه الشخصي، وإنما غايته كشف الحقيقة من أي سبيل يجده القاضي مؤديًا إليها وبدون رقابة عليه في ذلك سوي ضميره إذ ليس من حقه مسايرة أفكاره الخاصة في تقدير الأدلة فلا يجوز أن يكون تقدير الحكم حقلًا للأفكار الشخصية، فالمحكمة العليا تراقب صحة الدليل لا طريقة استخلاصه بماذا اقتنعت محكمة الموضوع وليس لماذا اقتنعت؟. ومن ثم فإن التفتيش للحاسوب يمكن أن يتم بغير نص في قانون الإجراءات الجنائية، بشرط أن يتم الحصول عليه بطريقة شرعية ونزيهة دون استخدام التدليس أو الغش أو الخداع [271]. لذلك من يتصرف على وجه مخالف للشرعية الجنائية يعد مقصرًا في عمله ومخالفًا في واجباته فيستحق المؤاخذة مع التعويض [272].

3. وجوب تحصيل الدليل بطريقة أمينة ونزيهة في البحث عن الحقيقة، سواء في مجال البحث عن الجرائم التقليدية، أم في مجال التنقيب في جريمة نشر الأخبار الكاذبة عبر وسائل التواصل الاجتماعي [273]، فرغم أن قانون الإجراءات الجزائية لا يتضمن أية نصوص تتعلق بمبدأ الأمانة أو النزاهة في البحث عن الحقيقة القضائية، إلا أن الفقه والقضاء يقرر هذا المبدأ، سواء في مجال التنقيب عن الأدلة الجنائية ومن بينها المخرجات الإلكترونية بطريقة شرعية ونزيهة، ويعد من الطرق غير المشروعة الحصول على الأدلة الإلكترونية الناتجة عن جريمة نشر الأخبار الكاذبة عبر وسائل التواصل الاجتماعي، باستخدام التدليس أو الغش أو الخداع، أو الإكراه المادي والمعنوي في مواجهة المتهم المعلوماتي من أجل فك شفرة نظام معلوماتي أو الوصول إلى ملفات البيانات المخزنة ... الخ، أو أن يستدعى المتهم المعلوماتي للتحقيق معه في توقيتات متأخرة ليلًا أو في ساعات

(271) أحمد. هلالي عبد اللاه (2008). *حجية المخرجات الكمبيوترية*. جمهورية مصر العربية: دار النهضة العربية. ص 121.
(272) زيدان. فاضل (2006). *سلطات القاضي الجنائي في تقدير الأدلة*. ص 107.
(273) أحمد. هلالي عبد اللاه (2008). *حجية المخرجات الكمبيوترية في الإثبات الجنائي*. ص121.

مبكرة من الصباح وبصفة متكررة، أو إطالة التحقيق لمدة طويلة بغية معرفة معلومات معينة حول قاعدة بيانات Data Base أو نظام إدارة البيانات أو خريطة تدفق البيانات أو قنوات إرسال البيانات أو التصميم التفصيلي للنظام المعلوماتي، أو المراقبة الإلكترونية عن بعد على شبكات الحاسب الآلي دون مسوغ قانوني معمول به مما يجعل الدليل غير مشروع.

4. يجب مراعاة حق الدفاع ومراعاة كل الظروف عند تقدير القيمة ووزن البيانات المستخرج عن طريق الحاسوب والمقبولة في الإثبات بالنسبة لكل قضية [274].

5. مشروعية الدليل بالإدانة أو بالبراءة: الرأي الأول: اشتراط المشروعية في دليل البراءة: إذا كانت الوسيلة غير المشروعة التي توصل بها إلى الدليل الإلكتروني؛ فإنه يتوجب إهدار ذلك الدليل، وعدم التعويل عليه، استنادًا إلى أن شرف الوسيلة ومشروعيتها في الوصول إلى الحقيقة يعد شرف مشروعية الغاية في الوصول للحقيقة. والعمل بغير ذلك يدمر الحقوق والحريات ويحرض على ارتكاب الجرائم توسلًا لإثبات البراءة. استنادًا إلى نص (المادة 190) من قانون الإجراءات الجزائية السعودي على أنه "لايترتب على بطلان الإجراء بطلان الإجراءات السابقة عليه ولا الإجراءات اللاحقة له إذا لم تكن مبنية عليه"، فالقاعدة هي أن الإجراء الباطل يمتد بطلانه إلى الإجراءات اللاحقة عليه إذا كانت هذه الإجراءات تترتب عليه مباشرة العمل بقاعدة استبعاد الدليل الجنائي الذي تم الحصول عليه بطريقة غير مشروعة سواء تم التوصل إليه مباشرة أو بطريقة غير مباشرة وكان متضمنًا اعتداءً على الحقوق الأساسية للمواطن فيتعين استبعاده من جلسة المرافعة حتى ولو كان دليلًا ملائمًا أو موضوعيًا أي يتصل بموضوع النزاع مباشرة فيتبعه أو يسهم في إثباته ولا تفرق النصوص ولا القاعدة بين دليل الإدانة ودليل البراءة فالقاعدة: "كل ما بني على باطل

(274) بدير. محمد ممدوح. (2019م). *مكافحة الجريمة المعلوماتية عبر شبكات الإنترنت والاستدلال كوسيلة لإثبات الجريمة المرتكبة عبر الإنترنت*. مصر: مركز الدراسات العربية. الطبعة الأولى. ص 170.

فهو باطل"[275]. إضافة إلى عدم تناول النص على مشروعية الحصول على دليل إثبات البراءة حتى لا نهدر مبدأ الشرعية لصالح البراءة فلا نصبغ المشروعية على البراءة التي تتأتى بدليل باطل كالشهادة الزور، ومن ثم فإن الدليل المستمد بطريقة مخالفة للأحكام الواردة في الدستور تكون باطلة بطلانًا مطلقًا لتعلقها بالنظام العام لحماية الحقوق والحريات الفردية منها طالما لم تتوفر فيه شروط حالات القبض ولا التفتيش ولا اتخاذ إجراءات الخبرة الجنائية، ويجوز لكل ذي مصلحة التمسك به، كما أن للمحكمة أن تقضي به من تلقاء نفسها، لأن ما يبنى على باطل يكون باطلًا كما ورد هذا القيد في (المادة 12) من الإعلان العالمي لحقوق الإنسان والمادة الخامسة منه التي حظرت التعذيب. وذهب الرأي الثاني، إلى عدم اشتراط المشروعية في دليل البراءة؛ ذلك أن البراءة تعد أصل في الإنسان، إذ أن عدم الاعتداد بالدليل غير المشروع إنما شرع ليضمن حرية المتهم، فلا يجوز أن ينقلب هذا الضمان ضده. وإن حق المتهم في تقديم الدليل يظل قائمًا مادام بقي الاتهام، ومتى لم يصدر حكم منهي لموضوع الدعوى بالقيود التي حددها القانون. وإن المتهم له الحرية الكاملة في اختيار وسائل دفاعه بقدر ما يسعفه مركزه في الدعوى. ويعلو حق المتهم في الدفاع عن نفسه على حق الهيئة الاجتماعية التي لا يضيرها تبرئة مُدان بقدر ما يؤذيها إدانة شخص برئ [276]، خصوصًا وترجع عدم مشروعية الدليل إلى أن وسيلة الوصول عليه تخالف قواعد الإجراءات الجزائية، فإنه يقبل في هذه الحالة الدليل الإلكتروني غير المشروع لإثبات البراءة، استنادًا إلى أن البطلان الذي شاب وسيلة التوصل إلى الدليل الإلكتروني غير المشروع، يرجع إلى فعل من قام بالإجراء الباطل؛ ومن ثم لا يجوز للمتهم أن يضار من فعل لا يد له فيه.

(275) بدير. محمد ممدوح (2019م). *مكافحة الجريمة المعلوماتية عبر شبكات الإنترنت والاستدلال كوسيلة لإثبات الجريمة المرتكبة عبر الإنترنت*. ص 172.

(276) بلال، أحمد عوض (2015م). *قاعدة استبعاد الأدلة المتحصلة بطرق غير مشروعة في الإجراءات الجنائية المقارنة*. ص259.

الشرط الثاني: يجب أن تكون الأدلة الإلكترونية يقينية وغير قابلة للشك:

يُشترط في الأدلة العلمية المستخرجة من الحاسوب الآلي وشبكة الإنترنت، أن تكون غير قابلة للشك للحكم بالإدانة بناء عليها إذا وصل اقتناع القاضي إلى حد الجزم واليقين بالقوة الاستدلالية على صدق نسبة الجريمة إلى شخص معين من عدمه لدحض قرينة افتراض البراءة؛ فيستطيع القاضي من خلال ما يعرض عليه من مخرجات إلكترونية، والانطباعات الذهنية من تصورات واحتمالات بالنسبة لها، أن يحدد قوتها الاستدلالية على صدق نسبة جريمة نشر الأخبار الكاذبة عبر وسائل التواصل الاجتماعي إلى شخص معين من عدمه. ونصت بعض قوانين الولايات في أمريكا، على أن النسخ المستخرجة من البيانات التي يحتويها الحاسوب تُعد من أفضل الأدلة المتاحة لإثبات هذه البيانات، ومن ثم يتحقق مبدأ اليقين لهذه الأدلة، والرأي السائد في الفقه هو اعتبار الأدلة الإلكترونية من مخرجات الحاسوب تحقق اليقين المنشود في الأحكام الجنائية، بشرط أن تكون البيانات دقيقة ونابحة عن الحاسوب بصورة سليمة لقبول الأدلة المستخرجة من الحاسوب التي تم تحويلها إلى الصورة المرئية، سواء كانت أصلًا أو كانت نسخًا مستخرجة عن هذا الأصل.

وقد نصت المادة (21) من قانون المعاملات الإلكترونية الأردني رقم (85) لسنة 2001م، التي جاء فيها بأن: (أ- يعد نظام المعالجة الإلكتروني مؤهلًا لإثبات تحويل الحق في السند تطبيقًا لأحكام المادة (20) من هذا القانون إذا كان ذلك النظام يسمح بإنشاء السند الإلكتروني وحفظه وتحويله وذلك بتوافر شروط...." وأنه في حالة عدم وجود نص على الدليل الإلكتروني ويخضع لمبدأين: مبدأ حرية إثبات الجرائم بكافة طرق الإثبات، ومبدأ القناعة الوجدانية للقاضي، ويدخل الدليل الإلكتروني في عناصر تكوين وجدان القاضي، الذي يخضع لمبدأ تساند الأدلة الذي يفيد اليقين وذلك حسب (المادة 121) من قانون الإجراءات الجزائية الإماراتي، والمادة 179 من نظام الإجراءات الجزائية السعودي رقم

(171) لسنة 1435 هـ والمادة (427) من قانون الإجراءات الجنائية الفرنسي على أنه "...باستثناء الحالات التي ينص عليها القانون، ويضفي القيمة القانونية على الأدلة التي يفرضها على القاضي بمقتضى ما يصدره من نصوص قانونية محددة فهو نوع من اليقين يتلقاه القاضي عن إرادة المشرع وهذا النوع من اليقين هو السائد في القانون[277]. أما اليقين الشخصي فيتمثل فيما يطمئن إليه وجدان القاضي ويرتاح إليه ضميره، أما اليقين القضائي فيستمد من الأدلة التي أقنعت القاضي، والذي يصل إليه – أي هذا اليقين – كما يصل إلى الكافة لأنه مبني على العقل والمنطق. ولذلك يقسم بعض الفقهاء القضاة في تقدير الدليل وبناء الحكم عليه إلى قاضٍ حاسم وقاضٍ متردد، وإلى قاضٍ حذر وقاضٍ غير مبال، وإلى قاضٍ موضوعي وقاضٍ منساق للتأثير النفسي [278]. إن القانون لا يسأل القضاة عن الوسائل التي كونوا بموجبها قناعاتهم، ولا يضع لهم القواعد التي يتبع لها كفاية الأدلة وتمامها وإنما يطلب منهم أن يسألوا أنفسهم في صمت وخشوع، وأن يبحثوا في صدق ضميرهم وإخلاصه عن الأثر الذي تركته في نفسهم الأدلة المقدمة ضد المتهم ووسائل دفاعه.

(277) قورة. نائلة عادل محمد فريد قورة (2005). *جرائم الحاسب الآلي* دراسة نظرية تطبيقية. لبنان: منشورات الحلبي. ص82.
(278) بهنام. رمسيس (1997). *علم النفس القضائي*. مصر: منشأة المعارف. ص31.

المطلب الثالث: جرائم نشر الاخبار الكاذبة ومشكلة الاختصاص

يطبق على جريمة نشر الأخبار الكاذبة عبر وسائل التواصل الاجتماعي ما يطبق على الجرائم المعلوماتية بصفة عامة، بوصفها فرع من أصل، وقد انقسمت التشريعات التي تعرف الجرائم الإلكترونية إلى نوعين؛ النوع الأول لم يحدد جهة قضائية مختصة؟ والثاني حدد تلك الجهة بنصوص خاصة. إلى النوع الأول ينتمي القانون الاتحادي رقم (34) لسنة 2021 بشأن مكافحة الشائعات والجرائم الإلكترونية إلى النوع الثاني وكذلك تنتمي له تشريعات كثيرة من الولايات المتحدة الأمريكية [(279)].

وفي ظل عدم تناول القانون الاتحادي رقم (34) لسنة 2021 بشأن مكافحة الشائعات والجرائم الإلكترونية لمسألة الاختصاص، فإنه لا مناص من اللجوء إلى القواعد العامة في تحديد المحكمة المختصة. وتقضي القاعدة العامة التي وضعتها المادة (142) من قانون الإجراءات الجزائية لدولة الإمارات العربية المتحدة بنظر الجريمة هي تلك التي وقعت الجريمة في دائرتها، وذلك بقولها "يتعين الاختصاص بالمكان الذي وقعت فيه الجريمة". وبناءً عليه فإن القواعد العامة يتعين أن تسري عند محاكمة مرتكب جريمة من جرائم تقنية المعلومات مثله في ذلك مثل أي جريمة أخرى، ومع ذلك فإن تطبيق معيار مكان وقوع الجريمة لا يخلو من بعض الصعوبات القانونية التي تجد تفسيرها في الطبيعة الخاصة للجريمة الإلكترونية. فما هو مكان وقوع الجريمة الإلكترونية؟ يلزم بادئ ذي بدء أن نذكر أن هناك طائفتين من الجرائم الإلكترونية؛ الطائفة الأولى وتضم الجرائم البحتة لتقنية المعلومات والنوع الثاني ويتضمن الجرائم التي تقع بطريق من طرق تقنية المعلومات. وتنتمي إلى النوع الأول من الجرائم جريمة التدخل والبقاء في النظام وجريمة إتلاف المعلومات والإخلال بسير النظام ... وتنتمي إلى النوع الثاني جريمة السب والقذف بطريق الإنترنت وجريمة النصب وجريمة غسل الأموال وجريمة الاستغلال الجنسي بالاستعانة بالإنترنت. في النوع

(279) بدير. محمد ممدوح. (2019م). *مكافحة الجريمة المعلوماتية عبر شبكات الإنترنت والاستدلال كوسيلة لإثبات الجريمة المرتكبة عبر الانترنت*. ص179.

الأول من الجرائم تقع الجريمة على جهاز معين يتداخل فيه المتهم أو يبقى فيه بطريقة غير مسموح بها، ومن ثم يمكن القول بأن الجريمة تقع في المكان نفسه الذي يقع فيه الجهاز المعتدي عليه مادام أن النشاط (الدخول أو البقاء) قد حدث في وقت تواجد الجهاز. بيد أنه قد يحدث أن يكون الدخول أو البقاء عن بعد من جهاز متواجد في مكان آخر. عندئذ يمكن القول بأن الجريمة تحدث في مكان وجود الجهاز المعتدي عليه وفي مكان وجود الجهاز الذي استعان به المتهم للقيام بالنشاط وهو الدخول أو البقاء المؤثم. هذا المكان الثاني قد يقع في إطار دائرة اختصاص المحكمة التي يقع فيها دائرتها الجهاز المعتدي عليه، عندئذ فلا تثار مشكلة قانونية [280]، وقد يقع هذا المكان في دائرة اختصاص محكمة أخرى بل قد يقع في خارج البلاد. في هذه الحالة الأخيرة يؤول الاختصاص وفقًا لمبدأ الإقليمية إلى محكمة الجهاز المعتدي عليه ومحكمة الجهاز الذي تم منه الدخول أو البقاء بالخارج.

وفي هذا المعنى تنص المادة (17) قانون الجرائم والعقوبات الاتحادي رقم (31) لسنة 2021 على أنه " تسري أحكام هذا القانون على كل من يرتكب جريمة في إقليم الدولة. ويشمل إقليم الدولة أراضيها وكل مكان يخضع لسيادتها بما في ذلك المياه الإقليمية والفضاء الجوي الذي يعلوها. وتعد الجريمة مرتكبة في إقليم الدولة إذا وقع فيها فعل من الأفعال المكونة لها أو إذا تحققت فيها نتيجتها أو كان يراد أن تتحقق فيها". أما بالنسبة للنوع الثاني من الجرائم والتي تنتمي أصلًا إلى الجرائم التقليدية ولكن الجديد فيها أنها تقع بطريق من طرق تقنية المعلومات، نقصد بالإنترنت، فإن الأمر يثير بعض الصعوبات القانونية فيما يتعلق بتحديد المحكمة المختصة [281].

(280) غنام. محمد غنام (2017). *دور قانون العقوبات في مكافحة جرائم الحاسب الآلي والإنترنت*. مصر: دار الفكر والقانون. ص 205.

(281) المصدر نفسه. ص 206.

المبحث الثالث: الإشكاليات المتعلقة بضبط مقترفي جريمة نشر الأخبار الكاذبة عبر وسائل التواصل الاجتماعي

للتعرف على الإشكاليات المتعلقة بضبط مقترفي جريمة نشر الأخبار الكاذبة عبر وسائل التواصل الاجتماعي، قام الباحث بتقسيم هذا المبحث إلى ثلاثة مطالب، وذلك على النحو الآتي:

المطلب الأول: التفتيش

تتكون نظم الحاسب الآلي من مكونات مادية Hardware ومكونات منطقية Software كما أنها تربطه بغيرها من الحاسبات شبكات اتصال على المستوى المحلى أو الدولى، لذا فقد ثار التساؤل الخاص بمدى قابلية مكونات وشبكات الحاسب الآلي للتفتيش؟ وما هى الضوابط التي يجب إتباعها في تلك الحالة؟ وهذا ما سوف نتناوله في هذا المطلب على النحو الآتي:

أولًا: مدى قابلية تفتيش المكونات المادية للحاسب الآلي

يعد تفتيش المكونات المادية للحاسب بأوعيتها المختلفة وصولًا للدليل الجنائي في جرائم المعلوماتية، مما يدخل في نطاق التفتيش طالما تم وفقًا للإجراءات القانونية المقررة.

وقد نظمت المادة 19 من اتفاقية بودابست تفتيش نظم الحاسب الآلي فبينت التزام كل دولة بالاتفاقية بإقرار الإجراءات التشريعية وغيرها من الإجراءات الأخرى، كلما كان ذلك ضروريًا، وذلك لتفويض سلطاتها المختصة بالتفتيش في، أو الدخول بالمثل على، ما يأتي:

أ- منظومة الكمبيوتر أو جزء منها وبيانات الكمبيوتر المخزونة بها.

ب- حجرة تخزين بيانات الكمبيوتر، والتى قد تكون بيانات الكمبيوتر مخزنة بها بأراضي الدولة الطرف بالاتفاقية.

ج- اتخاذ الإجراءات اللازمة لضمان أنه في حالة قيام سلطاتها بعمليات البحث أو الدخول بالمثل على منظومة كمبيوتر بعينها أو على جزء منها، وفقًا للفقرة (1) "أ"، ولديها أسباب للاعتقاد بأن البيانات المطلوبة مخزنة بداخل منظومة كمبيوتر أخرى أو بداخل جزء منها على أراضيها، وأن هذه البيانات يمكن الدخول عليها قانونًا من المنظومة الرئيسية أو متوافرة لها، فتصبح السلطات قادرة على توسيع عملية البحث بسرعة ونشاط أو الدخول بالمثل على المنظومة الأخرى. ومؤدى ذلك أن تفتيش تلك المكونات يتوقف على طبيعة المكان الموجودة فيه، وما إذا كان من الأماكن العامة أم الخاصة؟ إذ أن الصفة التي تنطلي على المكان لها أهمية خاصة في التفتيش، فإذا كانت موجودة في مكان خاص كمسكن المتهم أو أحد ملحقاته. فلا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش مسكنه، وبنفس الضمانات المقررة قانونًا في القوانين المختلفة [282]، وتتوقف حرمة المسكن بمدلوله الواسع والسابق تحديده على استمرار خصوصيته، فإذا أزال صاحب المسكن هذه الخصوصية وسمح للجمهور بغير تمييز بالتردد على هذا المكان، ارتفعت عنه الحرمة التي أضفاها القانون، ولا يجوز تفتيش مسكن المتهم ولا ملحقاته إلا بإذن قضائي مسبب.

وإذا كان الحاسب الإلكتروني أو الإنترنت موصولًا بسيارة، فإن حرمة السيارة الخاصة مستمدة من اتصالها بشخص صاحبها أو حائزها، فإذا كانت السيارة في حيازة الطاعن وتحت سيطرته قبيل الضبط، فإن ذلك يجعل له صفة أصلية عليها، ويضحى تفتيشها سليمًا في القانون. وبالرغم من أن محل العمل الخاص يتسم بالخصوصية حال قيام السلطات بتفتيش الحاسب في جرائم المعلوماتية، فإنه يجوز لسلطة التحقيق الحصول على رضاء صاحب العمل الموجود به الحاسب الإلكتروني محل الاعتداء وتفتيشه. ويتمتع أصحاب العمل في القطاع الخاص بسلطة واسعة في إبداء الموافقة على التفتيش في مقر العمل، ذلك أن التوقع المعقول للخصوصية، يضمن ما إذا كان مقر عمل الموظف الحكومي

(282) احمد. هلالى عبد الإله (2015). *تفتيش نظم الحاسب الآلي*. مصر: دار النهضة العربية. ص 74.

مفتوحًا بشكل كبير لزملائه الموظفين أو للعامة ولا يوجد لديه توقع معقول للخصوصية، فهذا المعيار يختلف بشكل واضح عن معيار التحليل المطبق في أماكن العمل الخاصة. إذ يتمتع موظفو القطاع الخاص بتوقع معقول للخصوصية في مقار عملهم، إذا لم يكن المكان متاحًا للكافة. وقدمت المحكمة العليا تصورًا للتفتيش بغير إذن في أماكن العمل الحكومية، وهو نموذج يطبق على تفتيش الحاسب الآلي [283]، حيث قضت في قضية o'connor بإجماع الآراء بأن موظف الحكومة يتمتع بالخصوصية في مقر عمله، ومع ذلك، فإن التوقع المعقول للخصوصية يصبح لا محل له إذا وجدت قواعد تسمح للمشرف على الموظف بالدخول إلى مكان عمل الموظف، فضلًا عن ذلك، فإن الرئيس في مقر العمل يمكن أن يقوم بالتفتيش بغير إذن حتى إذا كان التفتيش ينتهك توقع الموظف المعقول للخصوصية [284]، وبالنسبة للأماكن العامة، فإذا وجد الشخص في هذه الأماكن وهو يحمل مكونات الحاسب سالفة الذكر أو كان له السيطرة عليها أو الحيازة لها، فإن تفتيشها لا يكون إلا في الحالات التي يوجب القانون فيها تفتيش الأشخاص وبنفس الضمانات والقيود المنصوص عليها في هذا الصدد. ويجب على جهة التحقيق القائمة بالتفتيش في جرائم المعلوماتية التأكد من أن الحاسب الإلكتروني ينتفي عنه الخصوصية التي تحول دون القيام بالتفتيش، كما لو كانت المستندات الإلكترونية تتسم بسرية من شأن الإفصاح عنها إلحاق ضررًا بالغًا بالغير. فكلما كان لصاحب العمل سلطة فعليه في الاطلاع على بيانات المستند الإلكتروني المخزنة لدى مرؤوسيه، فإن شبهة الخصوصية تكون قد انتفت.

ففى قضية simons كان المتخصصون في الحاسب الآلي في قسم تابع لوكالة الاستخبارات المركزية قد علموا بأن موظفًا في الوكالة، يستخدم شاشة العرض بحاسوبه للحصول على صور منافية

(283) "actual office practices and procedures, or ….Legitimate regulation".
(284) see id, at 725 – 26 (o'connor, j, plurality opinion); id, at 732 (scalia, j, concurring).

للآداب العامة، وبما يشكل خرقًا لسياسة الوكالة. لذا قام هؤلاء المتخصصون بالدخول عن بعد إلى الحاسب الآلي الخاص به بغير إذن وحصلوا على نسخ لآلاف الملفات التي تحوي صور خزنها على القرص الصلب الخاص به. وعندما دفع المتهم ببطلان الدليل المستمد من التفتيش بدون إذن، رفضت المحكمة ذلك الدفع على سند من أن الاستخدام الرسمي للإنترنت الخاصة بأقسام CIA لا تتمتع بأي خصوصية تحول دون نسخ المستندات والملفات وانتهت إلى القضاء بإدانته، ومؤدى ما تقدم أنه متى قبل الموظف العام تداول المستند الإلكتروني عبر الإنترنت، فإن الخصوصية تنتفي عنه بما يجيز اعتراضه ونسخه والتحفظ عليه. وكأن المحكمة في ذلك الحكم قد اعتبرت قبول تداول المستندات الإلكتروني عبر الإنترنت دون تحفظ على خصوصيتها مشابهًا لمن يوجد في مكان عام يحق لمأمور الضبط القضائي ارتياده دون حاجة لإذن [285]. كما قضى القضاء الأمريكي بأن شبهة الخصوصية تنتفي عند استخدام سلطات الضبط لبرنامج الاستدعاء، لتضمنها أمرًا من مأمور الضبط بأن جميع المستندات محل الاستدعاء يجوز الاطلاع عليها. ومؤدى ذلك أنه يمكن لرئيس العمل ونائبه أن يقوموا بأنفسهم بتفتيش نظم الحاسب في جرائم المعلوماتية لدى مرؤوسيهم ولو تضمن التفتيش انتهاكًا للخصوصية' وقد أيدت المحكمة العليا هذا النهج في قضية o'connor عندما قضت أن رئيس العمل الحكومى أو نائبه يمكنهما تفتيش مقر العمل، – دون حاجة إلى إذن قضائى — حتى ولو تضمن التفتيش انتهاكًا للخصوصية طالما أن التفتيش كان له ما يسوغه قانونًا [286]. إلا أن القضاء الأمريكي قيد ذلك بقيد مهم وهو أن يكون الغرض من التفتيش الكشف عن الدليل في جريمة من جرائم الاعتداء على الحاسب الآلي، وأن تكون الإجراءات المتخذة قانونًا مرتبطة بأهداف التفتيش ارتباطًا ينأى به عن شبهة تجاوز حدود التفتيش. وتطبيقًا لذلك، قضى (بأن التفتيش عن البيانات الإلكترونية في الحاسب الآلي الخاص بالموظف لا ينطوى على شبهة

(285) عبد الحفيظ. أيمن. يناير 2004. حدود مشروعية أجهزة الشرطة فى مواجهة الجرائم المعلوماتية. مصر: ***مجلة مركز بحوث الشرطة***. العدد 25. ص380.

(286) see o'connor, 480 u.s.at 722 – 23 (plurality): id. At 732 (scalia, j… concurring).

التعسف أو التجاوز لاقتصار سلطات الضبط على تفتيش أسماء الملفات ثم تفتيش العناوين المشتبه فيها في زيارات متتابعة). ومن ثم، فإن تفتيش عنوان المشتبه فيه في تلك الحالة كان بعد ظهور دلائل كافية على ارتكابه جريمة من جرائم الاعتداء على الحاسب الآلي تسوغ قانونًا اتخاذ ذلك الإجراء.

ثانيًا: مدى قابلية خضوع المكونات غير المادية للحاسب الآلي للتفتيش:

إذا كان محل هذه الجرائم المكونات الغير مادية للحاسب وعلى رأسها برامجه أو بياناته، فإن الأمر يثير التساؤل حول إمكانية تطبيق قواعد التفتيش التقليدية بشأنها من عدمه؟ ويحاول بعض الفقه التغلب على هذه الصعوبة باللجوء إلى حيلة التمييز بين المعلومات وبين البيانات المعالجة آليًا. فينفى الطابع المادي عن أولها أو يؤكد للثانية طابعًا ماديًا على أساس أنها "نبضات أو ذبذبات الكترونية ...".

ومن ثم فأصحاب هذا الاتجاه ينفون الطابع المعنوي لهذه البيانات المعالجة آليًا مؤكدين أنها شئ يمكن لمسه في المحيط الخارجي، وأنها كيان مادي لا يمكن جحده مستندين في ذلك إلى حكم محكمة جنح بروكسل الذي أكد على كون هذه البيانات أشياء مادية محسوسة. وانتهوا إلى إمكانية خضوع هذه البيانات لقواعد التفتيش التقليدية، وبالتالى إمكانية ضبطها (287).

ويرى البعض أنه إذا كان الهدف من التفتيش هو ضبط الدليل المادى للإثبات الجنائى، فإن هذا المفهوم يمتد ليشمل الأدلة الإلكترونية بمختلف صورها. فالمادة 251 من قانون الإجراءات الجنائية اليونانى تعطى سلطات التحقيق إمكانية القيام بأى شئ يكون ضروريًا لجمع وضبط الدليل، ولذلك، فإن تفتيش وضبط المستندات الإلكترونية المخزنة في الذاكرة الداخلية للحاسب لا يشكل أية مشكلة في القانون اليونانى إذ بمقدور المحقق أن يعطي أمرًا للخبير بجمع البيانات التي يمكن أن تكون مقبولة كدليل في المحاكمة الجنائية. كما نصت المادة 19 من اتفاقية بودابست على أن تقوم كل دولة طرف بالاتفاقية

(287) يونس. حسين عبد الكريم. الجندي. خليل. يوسف.(2021). *الابتزاز الالكتروني والجرائم الإلكترونية* "المفهوم والأسباب". الأردن: دار كفاءة المعرفة. ص63.

بإقرار الإجراءات التشريعية وغيرها من الإجراءات الأخرى، وذلك لتفويض سلطاتها المختصة بالتفتيش في منظومة كمبيوتر بعينها أو على جزء منها. بينما اتجه البعض إلى أن الهدف من التفتيش لا يسرى على الأدلة الإلكترونية غير المادية ويقترح هذا الرأي لمواجهة هذا القصور التشريعي ضرورة أن يضاف إلى هذه الغاية التقليدية عبارة الأدلة الإلكترونية المعالجة عن طريق الحاسب الآلي، أو بيانات الحاسب الآلي، وبذلك تصبح الغاية الجديدة من التفتيش بعد هذا التطور الفني الحديث هي (البحث عن الأدلة المادية الإلكترونية) (288).

ثالثًا: مدى خضوع شبكات الحاسب الآلي للتفتيش في جرائم المعلوماتية

يظهر هذا الفرض في مجال الجرائم التي ترتكب باستخدام الشبكات، بحيث يتم ارتكاب الجريمة من أي من أجهزة الحاسب الآلية الأخرى والمتصلة بالحاسب الذي ارتكبت الجريمة في نظامه المعلوماتي. وفى هذا الفرض، فإن إجراءات التفتيش والضبط تتطلب الدخول في نظام معلوماتي لشخص آخر. فيثور التساؤل حول أثر تفتيش الأنظمة المتصلة بالنظام المأذون بتفتيشه إذا تواجدت في دوائر اختصاص مختلفة، هل يمتد تفتيش كمبيوتر معين إلى الأجهزة المرتبطة به داخل البلاد؟ وفى هذه الصورة يمكن التفرقة بين الفرضين الآتيين:

الفرض الأول: اتصال حاسب المتهم بحاسب موجود في مكان آخر داخل الدولة:

حيث أجازت بعض التشريعات المقارنة حلًا لهذه المشكلة، مثل الولايات المتحدة أن يمتد إذن التفتيش الصادر لمقر شركة معينة إلى فروعها الكائنة في العقار نفسه (289).

وتسمح الاتفاقية الأوروبية لجرائم الإنترنت لعام 2001 للدول الأعضاء أن تمد حدود التفتيش الذي كان محله جهاز كمبيوتر محدد إلى غيره من الأجهزة المرتبطة به في حالة الاستعجال، إذا كان يوجد

(288) يونس. حسين عبد الكريم، الجندي. خليل. يوسف. (2021). *الابتزاز الالكتروني والجرائم الإلكترونية*. ص155.

(289) Convention sur la cyberciminalité Budapest, 23. XI. 2001 Article no 19.

به معلومات يتم الوصول إليها في هذا الجهاز عن طريق الجهاز محل التفتيش. حيث إن المادة 19 من القسم الرابع تنص على أنه: "من حق السلطة القائمة بتفتيش الكمبيوتر الموجود في حيز اختصاصها أن تمد في حالة الاستعجال نطاق التفتيش إلى أي جهاز آخر، إذا كانت المعلومات المخزنة يتم الدخول إليها من الكمبيوتر الأصلي محل التفتيش"[290].

الفرض الثاني: اتصال حاسب المتهم بحاسب في مكان آخر خارج الدولة:

قد يكون من الضروري أثناء التحقيقات تفتيش جهاز كمبيوتر متواجد في الخارج كما لو تعلق الأمر بشركة وفروعها في الخارج، حيث ترتبط أجهزة الشركة بعضها ببعض وأحيانًا ترتبط بعض الأجهزة بقاعدة بيانات متواجدة في الخارج.

فقد نصت المادة 41 من اتفاقية تربس TRIPS على إلزام الأعضاء أن يتخذوا إجراءات الإنفاذ التي تتيح اتخاذ تدابير فعالة ضد أفعال التعدي بما في ذلك التدابير السريعة للحيلولة دون التعديات والتدابير التي تشكل رادعًا لأى تعديلات أخرى، ومن بين التدابير الرئيسية المطلوبة لاستحداث معدلات ردع أكثر فعالية ضد أفعال النسخ الرقمية غير المرخص بها، اتخاذ إجراءات سريعة بالتفتيش دون علم الطرف الآخر، وهو أمر ضروري للاحتفاظ بأدلة النسخ غير المشروعة للأعمال المخزنة إلكترونيًا في وسائط الكترونية يمكن سحبها بسهولة، وتطبيقًا لذلك، صدرت عن المجلس الأوروبي توصيات تجيز أن يمتد تفتيش الكمبيوتر إلى الشبكة المتصل بها، ولو كانت تلك الشبكة تقع خارج إقليم الدولة. فتنص التوصية رقم 13 لسنة 1995 المتعلقة بالمشكلات القانونية لقانون الإجراءات الجنائية المتصلة بتقنية المعلومات، على أنه لسلطة التحقيق عند تفتيش المعلومات وفقًا لضوابط معينة، أن تقوم بمد مجال تفتيش كمبيوتر معين يدخل في دائرة

(290) الكتبي. آمنة جمعة. (2012). "أثر الشبكات الاجتماعية على التواصل الاجتماعي". ***الفكر الشرطي***. الإمارات: ص85.

اختصاصها إلى غير ذلك من الأجهزة ما دامت مرتبطة بشبكة واحدة وأن تضبط البيانات المتواجدة فيها، ما دام أنه من الضروري التدخل الفوري للقيام بذلك [291].

وتجيز بعض التشريعات تفتيش الأنظمة المتصلة حتى ولو كانت متواجدة خارج إقليم الدولة فتجيز المادة 17 فقرة 2 من قانون الأمن الداخلي الفرنسي لمأموري الضبط القضائي أن يقوموا بتفتيش الأنظمة المتصلة، حتى ولو تواجدت في خارج الإقليم مع مراعاة الشروط المنصوص عليها في المعاهدات الدولية [292].

وقد أطردت أحكام القضاء الأمريكي على أنه إذا كان الإذن صادرًا لتفتيش جهاز الكمبيوتر في موضعه، فإن هذا الإذن يسمح بتفتيش ملحقات الجهاز من أدوات مثل الطابعة والديسكات والأقراص الممغنطة. ومما يؤيد أن الإذن بضبط وتفتيش ملفات معينة يشمل ضبط وتفتيش الجهاز بأكمله، أن بعض الأجهزة محمية بكلمات مرور، الأمر الذي يقتضي ضبط الجهاز بأكمله للتغلب على هذه العقبة من الناحية الفنية. وقد أعترف القضاء الأمريكي بهذه الضرورة العملية في أحكامه [293]، ويرى جانب من شراح القانون ضرورة أن يتصف الإذن الصادر بالتفتيش بالمرونة من حيث إتاحة مساحة واسعة لمأموري الضبط في تنفيذ إذن التفتيش ولكن بضوابط معينة، بحيث لا يتجاوز ذلك إلى الهدف المقصود من صدور الإذن عن طريق تحديد مجال هذا التفتيش، وما يستتبعه بالضرورة من تتبع من خلال شبكات المعلومات، إذا كان لذلك ضرورة. ويخضع تقدير ذلك لسلطة القاضي التقديرية من حيث توافر حالة الضرورة أم عدم توافرها بحيث يكون إذن التفتيش متضمنًا الآتي: البحث عن أدلة محصلة من كيان الحاسب المنطقي والتى يدخل فيها برامج التطبيق ونظام التشغيل [294].

---

(291) مصطفي. أحمد محمود محمد. (2014). "الاثبات الإلكتروني في الجرائم المعلوماتية". ***مجلة كلية الدراسات العليا***. أكاديمية الشرطة المصرية. العدد 31. ص ص227 – 228.

(292) Loi 18 Mars 2013 pour la securite Interieure Article 17l2.

(293) القحطاني. منصور بن ناصر محمد. (2015). ***الحماية الجنائية للخصومة من تأثير النشر من خلال وسائل الإعلام في القانون القطري***. **"دراسة مقارنة"**. (رسالة دكتوراه). مصر. جامعة القاهرة. ص40.

(294) المصدر نفسه. ص52.

أ- البيانات المستخدمة بواسطة برنامج الحاسب أو كيانه المنطقى.

ب- السجلات التي تثبت استخدام الأنظمة الآلية لمعالجة البيانات.

ج- السجلات المستخدمة في عملية الولوج في النظام الآلي لمعالجة البيانات [295]، ومن ثم يتضح إلى أي مدى يحتوي إذن النيابة على مرونة تمكن مأموري الضبط القضائي من مباشرة أعمالهم.

فمن المبادئ المقررة أنه إذا قام مأمور الضبط القضائي بتفتيش أشياء لم يحددها الإذن الصادر بالتفتيش، فإن ذلك يصم التفتيش بالبطلان. وذلك استنادًا إلى أن القائم بالتفتيش قد خالف الإذن بالتفتيش.

المطلب الثاني: المعاينة

يعتمد ضبط جريمة نشر الأخبار الكاذبة عبر وسائل التواصل الاجتماعي وإثباتها في المقام الأول على جمع الأدلة التي تكشف عن مقترفها، فلا يمكن الوصول إلى براءة المتهم أو إدانته إلا من خلال الأدلة التي من شأنها أن تولد القناعة لدى القاضي بالبراءة أو بالإدانة، وقد حصر المشرع وسائل إثباتها؛ وذلك لما فيها من مساس بحرية الأفراد وحقوقهم الأساسية، فلا يجوز أن تخرج الأدلة التي يتم تجميعها عن تلك التي اعترف لها المشرع بالقيمة القانونية [296].

وتعد المعاينة من المراحل الأولى للاستدلال حول ملابسات الجريمة بل ومن أهمها على الإطلاق؛ نظرًا لقدرتها على توفير أدلة إثبات الجريمة. وبظهور نوع جديد من الجرائم يعتمد في المقام الأول على شبكة المعلومات الدولية، كما في جريمة نشر الأخبار الكاذبة عبر وسائل التواصل الاجتماعي، وما نجده فيها من اختلاف في طبيعة السلوك الإجرامي، مما يستوجب ابتكار إجراءات خاصة بالمعاينة في هذا المجال [297].

---

(295) شيماء عبد الغنى عطا الله (2015). *الحماية الجنائية للتعاملات الالكترونية*. مصر: دار النهضة العربية. ص 318

(296) السوليه. أحمد يوسف محمد (2016). الدليل الرقمي ودوره في الإثبات الجنائي. أكاديمية الشرطة المصرية. كلية الشرطة. ***مجلة البحوث القانونية***. العدد 8. ص198.

(297) الكواري. محمد علي.2007م. *مسرح الجريمة ودوره في كشف غموض الجريمة*، السعودية: جامعة نايف العربية للعلوم الأمنية. ص44.

أولًا: المفهوم العام للمعاينة

تعني المعاينة رؤية أماكن ارتكاب واقعة الجريمة، كما تتجه إلى فحص جسم المتهم والمجني عليه، وإثبات ما يوجد فيهما من آثار[298]، وقد عرفها جانب من الفقه بأنها "إثبات مباشر ومادي لحالة الأشخاص والأماكن ذات الصلة بالحادث، عن طريق رؤيتها وفحصها حسيًا؛ للكشف عن حقيقة الجريمة ومرتكبها"، ويتضح من ذلك أن جوهر المعاينة يكمن في الملاحظة والفحص الحسي المباشر لمكان أو شخص أو أي شيء له علاقة بالجريمة.

ويجوز الالتجاء إلى المعاينة في كافة الجرائم، وهو إجراء هادف غايته كشف وصيانة العناصر المادية التي تتعلق بالجريمة، وتفيد في التحقيق الجاري بشأنها، فإذا انعدمت جدواها بالنسبة للتحقيق لم يكن ثمة مجال أو مقتضى لإجرائها، وذلك كما في جريمة القذف والسب التي تقع في غير العلانية، وغيرها من الجرائم على ذات الشاكلة.

ثانيًا: أهمية المعاينة:

ينتج عن إجراء المعاينة الحصول على كم هائل من المعلومات الكاشفة عن غموض الجريمة المرتكبة، والتي تتمثل فيما يلي[299]:

1- إثبات وقوع الجريمة، وتوافر أركانها القانونية.

2- المصدر الرئيسي للأدلة التقليدية، فهي تكشف عن آثار خاصة بالجاني، وما تخلف عنه أثناء ارتكابه الجريمة، والأدوات المستعملة فيها.

3- التعرف على أسلوب ارتكاب الجريمة، والذي يفيد في تحديد الاشتباه فيمن قام بتنفيذها.

---

(298) بدير. محمد ممدوح. 2019. *مكافحة الجريمة المعلوماتية عبر شبكات الإنترنت والاستدلال كوسيلة لإثبات الجريمة المرتكبة عبر الإنترنت*. ص120.

(299) محمد محمد عنب، "المعاينة في الإثبات الجنائي"، مقال منشور. ***مجلة الأمن والحياة***، جامعة نايف العربية للعلوم الأمنية، العدد رقم (390)، الرياض، 2014م، 380 وما بعدها.

4- نقل الحدث – الجريمة – من الماضي إلى الحاضر، وهو ما يسهل من رؤيتها بشكل واضح، والتعرف على خباياها.

ثالثًا: مفهوم معاينة مسرح الجريمة الإلكترونية

يقصد به معاينة الآثار التي يتركها مستخدم الحاسب الآلي أو الإنترنت، وتشمل الرسائل المرسلة منه أو التي يستقبلها، وكافة الاتصالات التي تمت من خلال الحاسب الآلي وشبكة الإنترنت.

ويلاحظ أن الآثار المعلوماتية أو الرقمية المستخلصة من أجهزة الحاسب الآلي تكون ذات قيمة جنائية مهمة فيما تحتويه من معلومات تساعد على الوصول لشخصية الفاعل، وذلك كما في صفحات المواقع المختلفة Web Pages[300].

رابعًا: مسرح جريمة نشر الأخبار الكاذبة عبر وسائل التواصل الاجتماعي

يتمتع مسرح الجريمة ومستودع سرها الأول بأهمية كبيرة؛ نظرًا لما يحتويه من آثار هي في حقيقة الأمر مفاتيح لحل لغز الكثير من الجرائم الغامضة، ويعرف بالمكان الذي ارتكبت فيه الجريمة أو أجزاء منها، وقد يتكون من عدة أماكن؛ وفقًا لكل جريمة وعناصرها، والمراحل التي مرت بها منذ التخطيط والإعداد لها حتى تنفيذها ومحاولة إخفاء معالمها، وتتباين مسارح الجريمة في شكلها العام من جريمة إلى أخرى، وذلك بقدر اختلاف عناصر وأدوات تنفيذ كل جريمة على حدة[301].

ويجب عند الشروع في جمع الأدلة من مسرح جريمة نشر الأخبار الكاذبة عبر وسائل التواصل الاجتماعي التعامل معه على أنه مسرحان للجريمة، وذلك كما يلي:

- مسرح جريمة تقليدي:

يقع خارج بيئة الحاسوب، ويتكون بصفة رئيسية من المكونات المادية المحسوسة للمكان الذي تمت فيه

(300) ممدوح. خالد (2009). *فن التحقيق الجنائي في الجرائم الإلكترونية*. مصر: دار الفكر الجامعي. ص86.
(301) الدسوقي. طارق إبراهيم (2012). *فن التحقيق الجنائي في الجرائم الإلكترونية*. مصر: دار الجامعة الجديدة. ص45.

الجريمة، وما قد يتركه فيه الجاني من آثار عديدة، كالبصمات، أو المتعلقات الشخصية، أو وسائط التخزين الرقمي، أو غيرها، ويتعامل الفريق كل حسب اختصاصه.

- مسرح جريمة سيبراني(302):

يقع داخل بيئة الحاسب الآلي، ويتكون من البيانات الرقمية التي تتواجد وتنقل داخله وداخل شبكاته أيضًا، والمتواجدة في ذاكرته، وفي الأقراص الصلبة، ويكون التعامل معها من خلال الخبراء المتخصصين في مجال الأدلة الرقمية التي من هذا النوع.

خامسًا: أهمية المعاينة في جريمة نشر الأخبار الكاذبة عبر وسائل التواصل الاجتماعي:

تكمن أهمية المعاينة بالنسبة للجرائم التقليدية في أنها تحتل مكانة الصدارة على غيرها من الإجراءات الاستدلالية الأخرى؛ وذلك بحسب المركز المحوري لدورها في تخيل طريقة ارتكاب الجريمة، وظروفها وملابساتها، وإتاحة الأدلة المادية والتنسيق فيما بينها على ضوء المعلومات التي تتضمنها، وبما يكفل التخطيط الصحيح لعمليات البحث الجنائي، إلا أن دورها في إطار كشف غموض جريمة نشر الأخبار الكاذبة عبر وسائل التواصل الاجتماعي ليس بذات الدرجة من الأهمية؛ ويرجع السبب في ذلك إلى أن جريمة نشر الأخبار الكاذبة عبر وسائل التواصل الاجتماعي قلما تخلف عند ارتكابها آثار مادية، حيث يكون عدد كبير من الأشخاص قد تردد على مكان أو مسرح الجريمة خلال المدة الزمنية التي مرت بين ارتكاب الجريمة واكتشافها، مما يتيح مجالًا واسعًا لحدوث تغيير، أو إتلاف، أو زوال، أو عبث بالآثار المادية، الأمر الذي يؤدى إلى الشك من الدليل المستقي من المعاينة.

وينبغي لتجنب تلك السلبيات، وحتى تكون المعاينة في جريمة نشر الأخبار الكاذبة عبر

(302) "الجريمة السيبرانية" هو مصطلح مشتق من مصطلح "الفضاء السيبراني Cyber Space" ويعني المجال الافتراضي الذي يعتمد على نظم الحاسبات وشبكات الإنترنت ومخزون هائل من المعلومات والبيانات، بحيث يتم الاتصال بالشبكات عبر الحاسبات، أو الهواتف، أو غيرها من الأجهزة الذكية، ومن دون تقيد بالحدود الجغرافية، لمزيد من التفاصيل راجع:

- PW Singer, Cyber security and cyberwar, Oxford university press, New York, 2014, p.107.

شبكات التواصل الاجتماعي لها فائدة في كشف حقيقتها ومعرفة مرتكبها، مراعاة عدد من القواعد والإرشادات الفنية، يمكننا إبرازها في النقاط الآتية [303]:

أ. تصوير الحاسب الآلي والأجهزة الطرفية المتصلة به، مع مراعاة تسجيل وقت، وتاريخ، ومكان كل صورة.

ب. ملاحظة طريقة إعداد النظام بعناية.

ج. مراقبة وإثبات الحالة التي توجد عليها التوصيلات والكابلات المتصلة بكل مكونات النظام؛ حتى يمكن إجراء عمليات المقارنة والتحليل عند العرض على المحكمة فيما بعد.

د. عدم رفع أية مادة معلوماتية من مسرح الجريمة قبل عمل اختبارات التأكد من خلو المحيط الخارجي لموقع الحاسب الآلي من أي مجال مغناطيسي يمكن أن يتسبب في حذف البيانات المحفوظة.

هـ. التحفظ على المعلومات الموجودة في الأوراق الممزقة بسلة المهملات، والشرائط والأقراص المدمجة غير السليمة، وفحصها، ورفع البصمات الموجودة عليها.

و. التحفظ على مستندات الإدخال، والأوراق المطبوعة من الحاسب الآلي التي لها صلة بالجريمة؛ لرفع ومضاهاة أي بصمات قد توجد عليها.

ز. قصر القيام مباشرة بإجراءات المعاينة على المحققين الذين يتمتعون بالكفاءة العلمية، والخبرة الفنية في مجال التعامل مع الحاسبات الآلية.

ويتم توثيق مسرح الجريمة ووصفه بشكل جيد، كما يتم توثيق كل دليل على حدة بما فيها الأدلة الرقمية، بحيث يتم إيضاح مكان الضبط، والهيئة التي كان عليها، ومن القائم برفع الدليل وتحريزه، وكيف ومتى حدث ذلك؟ بل يرى البعض أن التوثيق يجب أن يشتمل على جميع المصادر الموجودة على

(303) بدير. محمد ممدوح (2019). *مكافحة الجريمة المعلوماتية عبر شبكات الإنترنت والاستدلال كوسيلة لإثبات الجريمة المرتكبة عبر الإنترنت*. ص123.

الشبكة التي ترتبط بها الأجهزة محل التحقيق، ولعله من أبرز الأشياء التي يحتمل وجود الأدلة الجنائية المرتبطة بجريمة نشر الأخبار الكاذبة عبر وسائل التواصل الاجتماعي فيها هي الآتي:

الأوراق:

رغم أن ظهور أجهزة الحاسب الآلي قد قلل من حجم الملفات الورقية التقليدية التي تستخدم في حفظ البيانات والمعلومات، إلا أننا نجد العديد يقومون بطباعة المعلومات؛ لمراجعتها، أو للتأكد من الشكل العام للمستند، أو الرسالة، أو الرسومات، ومن ثم فهذه المطبوعات تعد من الأدلة التي يجب مراعاتها في البحث الجنائي أثناء المعاينة.

جهاز الحاسب الآلي وملحقاته:

من البديهي أن وجود جهاز حاسب إلى مهم جدًا للقول بأن الجريمة الواقعة هي جريمة نشر الأخبار الكاذبة عبر وسائل التواصل الاجتماعي بواسطة شبكة الإنترنت، وأنها مرتبطة بالمكان أو بالشخص الحائز لهذا الجهاز، ولأجهزة الحاسب الآلي أشكال وأحجام متباينة؛ لذا فإن خبير الحاسب الآلي وحده هو الذي يستطيع أن يتعرف على مواصفاته بدقة وسرعة.

البرمجيات:

ينشأ الدليل الرقمي باستخدام برامج خاصة يكون استخدامها – عادةً – ليس واسع الانتشار، وإن كان ضبط الأقراص المستعملة بغرض تثبيت وتنصيب هذه البرامج يعد أمرًا في غاية الأهمية عند فحص الأدلة.

وسائط التخزين المتحركة:

تعد هذه الوسائط جزءًا من الجريمة متى كانت محتوياتها عنصرًا من عناصرها، ومن أمثلتها: الأقراص المدمجة (أقراص الليزر)، والأقراص المرنة، والأشرطة المغناطيسية، وغيرها.

المودم Modem:

هو الوسيلة التي تمكن أجهزة الحاسب الآلي من الاتصال ببعضها البعض عبر خطوط الهاتف، وفي الوقت الحالي تطور ليكون جهاز إرسال واستقبال، وإجراء المكالمات الهاتفية، وتبادل البيانات وتعديلها.

المطلب الثالث: إشكالية إثبات جرائم نشر الأخبار الكاذبة عبر الإنترنت

رغم أن انتشار الأجهزة المحمولة باليد والمتصلة بشبكات اللاسلكي يعد بمثابة نقلة نوعية في عصر الحاسب الآلي، إلا أنه اعتبر أحد أهم تحديات البحث والتحقيق في الأنشطة الإجرامية في مجال أجهزة الحاسب الآلي المنتشرة على مستوى العالم، وتمثلت هذه الصعوبات في كيفية الحصول على كافة الأدلة من هذه الأجهزة ذات العلاقة بالواقعة محل البحث الجنائي.

وتسهم عدة عوامل على وجه العموم في هذه الإشكالات أو التحدي، وذلك على النحو الآتي:

أ. ينتج عن طبيعة الشبكات الموزعة توزيعًا لمسارح الجريمة توزيعًا للدليل الإلكتروني في عدة أماكن مختلفة مما يؤدي إلى مشاكل عملية وتشريعية خصوصًا مع اختلاف القوانين فعلى سبيل المثال وفي أغلب الحالات قد لا يكون ممكنًا الحصول على الأدلة من أجهزة الحواسب الموجودة في دولة أخرى، وحتى في حالة وجود إجراءات دولية، والتي من شأنها تسهيل عملية تبادل الأدلة الرقمية حيث إن معظم هذه الأجهزة معقدة، وهي ليست عملية إلا بالنسبة للجرائم الخطيرة نتيجة لذلك يبحث المحقق المعلوماتي عن أفضل الأساليب لطلب واستدعاء المعلومات بصورة رسمية من الدول الأخرى.

ب. الصعوبات المتمثلة في طبيعة البيانات الرقمية نفسها التي يمكن مسحها أو تغييرها بسهولة لذلك من الضروري جمعها والاحتفاظ بها بسرعة كلما أمكن، وإذا كان المرور بالشبكات لا يستغرق إلا جزءًا

من الثانية وهي فترة قصيرة جدًا ونظرًا لحجم الملفات الكبيرة فإنه لا يجوز احتجاز تلك الملفات إلا لأيام قليلة. (304)

إضافة إلى أنه إذا كان المجرمون لديهم المهارات والفرص فإنهم يدمرون الأدلة أو يحرفونها أو يعدلونها لحماية أنفسهم، ويكمن ثالث هذه العوامل في هذا التحدي الكبير في الحجم المطلوب في الخبرة الفنية حيث إنه يوجد تباين واختلاف بين شبكة وأخرى عند دمج تقنيات مختلفة في أساليب فريدة من نوعها، فإنه لا يوجد شخص واحد مجهز ومؤهل للتعامل مع كافة المواقف، لذلك فإنه من الضروري وجود أشخاص لديهم الكفاءة للتعامل مع تقنية محددة قبل الحصول على الأدلة، أما رابع هذه العوامل فهو حجم البيانات الضخمة التي غالبًا ما تستخدم في التحقيق من خلال أنظمة الحاسب الآلي، فعملية البحث عن الأدلة اللازمة للإدانة أو البراءة في كم كبير من البيانات الرقمية هي عملية بالغة الصعوبة وتتطلب جهدًا ومهارة عالية.

والبيانات الرقمية المتحصلة من شبكات المعلومات، تعد بيانات متحركة كبعض التطبيقات التي تسمح للشخص بتحميل ملفاته على الشبكة العالمية للمعلومات، ويمكن لأي شخص الحصول على نسخة من تلك الملفات، ولتوضيح طبيعة الصعوبة التي تواجه الخبير الإلكتروني عند جمع الأدلة من شبكات المعلومات، نبين عددًا من هذه المشكلات على النحو الآتي:

1- الشبكات وإخفاء الهوية:

تواجه عملية جمع الأدلة الجنائية الرقمة من مسرح الحادث مشكلة أخرى تتمثل عند تعمد المستخدم إخفاء هويته Encryption، وينشأ عن ذلك مزيد من التحديات الأمنية عندما لا يبذل المجرمون جهدًا

(304) الغفلي. محمد خليفة (2021). *حجية الدليل الرقمي في الإثبات الجنائي*. ص383.

في إخفاء هويتهم، فإنهم يستطيعون الادعاء بأنهم لم يكونوا مسئولين عن ذلك [305]، ويتخذ المجرمين بعض الإجراءات لإحباط محاولة اعتقالهم، ذلك في حالة بذلهم قدرًا ضئيلًا من الجهد المطلوب لطمث هويتهم على شبكة المعلومات الدولية الإنترنت لكي تظل أنشطتهم مجهولة ومن هذه الإجراءات ما قد يكون بسيطًا مثل استخدام حاسب آلي بمكتبة عامة، إلا أن هناك العديد من البرامج والتطبيقات التي تقدم وسائل متباينة في كيفية طمث الهوية على شبكة "الإنترنت" مما يعمل على تفاقم الموقف بالنسبة للمحق الجنائي أو خبير الأدلة الرقمية.

وتقدم عملية الإخفاء تحديًا آخر هامًا، حيث يجعل الأمر صعبًا أو مستحيلًا على الفاحصين القائمين على تحليل الأدلة التي تم العثور عليها وتجميعها وإدراجها بمستندات والاحتفاظ بها [306]، فهناك عدة طرق لحل رموز الإخفاء أو التحايل عليها كما ظهر في حالة Scarfo، المثيرة للجدل حيث حصل المحققون على تصريح باستخدام أساليب استرداد من شأنها انتزاع المعلومات الضرورية ذات الصلة بالمفاتيح والملفات المخفية، وذلك أثناء عملية التحقيق في ملهى للمقامرة غير المشروعة، والاحتيال على الحصول على قرض فقد اكتشف المحققون كلمة السر المؤدية إلى مفتاح اسكاريو PGP، الخاص بالملهى وبعد ذلك استخدموا هذه الكلمة في حل رموز البيانات الخاصة به وذلك من خلال القيام بصورة سرية بمراقبة كل ما طلبه الملهى حتى أمكنهم الحصول على كافة المعلومات اللازمة للإدانة[307].

2- الشبكات وإخفاء المعلومات:

تضع عملية إخفاء المعلومات Steganography تحديات مماثلة لخبراء الأدلة الرقمية، مما يجعل الأمر صعبًا أو مستحيلًا للعثور على البيانات الرقمية وهناك العديد من الاتجاهات المختلفة فيما يتعلق بإخفاء

(305) مصطلح Encryption يعني تشفير أو إخفاء، وهي عملية تشفير للبيانات لمنع الولوج غير المرخص لها، وخاصة أثناء عمليات نقل البيانات، وتعتمد عملية الإخفاء بشكل أساسي على مفتاح مهم جدًا من أجل فك تشفير البيانات، ولقد ابتدع المكتب الوطني الأمريكي للمقاييس مقياسًا معقدًا للإخفاء وأسماء مقياس تسمية البيانات Des وهو يعني عددًا غير محدد من طرق الإخفاء للبيانات.

(306) Wigler R.D, US District coint. District of New Jersey. https://epic.org/crypto/scarfo/gov_ex_parte_mot.pdf.

(307) يعد برنامج Pretty Good Privacy (PGP) من أشهر وأقوى البرامج العاملة في هذا المجال.

البيانات حيث يمكن الجمع بين إخفاء الهوية Encryption إخفاء المعلومات Steganography، أو البيانات المخفية لإنشاء نظام بيانات آمن تجعل عملية استعادة الأدلة وإعادة تركيبها أمرًا في غاية الصعوبة إلا أنه توجد بعض البرامج والأنظمة التي يمكنها مواجهة تلك المشكلة مثل النظام المعروف باسم Marutukku الذي يعمل على استعادة كافة البيانات والملفات المخفية.

ومن جهة أخرى يستطيع أي مهاجم من الناحية النظرية أن يقوم بفحص الخصائص المغناطيسية Ferrite Coating الذي يكسو سطح القرص لكي يحدد عدد المرات أي برنامج بالقراءة أو الكتابة في أي جزء من القرص الصلب Drive، يسمح ذلك لمهاجم بتخمين عما إذا كانت هناك أي مساحة خالية على القرص Disk، أو تحتوي على بيانات مخبأة Hidden Data، وفي حالة استطاعة المهاجم حل رموز الإخفاء على سبيل المثال فإنه باستطاعته أن يضع خريطة لأجزاء القرص المستخدمة مرارًا على خريطة خاصة بخريطة توضح الأجزاء المستخدمة وغير المستخدمة وفي حالة رؤيته جزءًا غير مستخدم قد تم الدخول عليه بصورة متكررة سواء بغرض القراءة أو الكتابة فإنه يستطيع التخمين بأن هناك احتمال أكثر لوجود بيانات أو معلومات مخبأة يمكنه حينها من الاطلاع عليها(308).

3- أنواع البيانات المتحركة المحفوظة على شبكات المعلومات:

ولتوضيح طبيعة البيانات المتحركة نوضح أربعة أنواع من البيانات، كل نوع منها يختلف عن الآخر في طريقة تكوينه وانتشاره، وتحركاته على شبكات المعلومات، وذلك على النحو الآتي:

أ- البريد الالكتروني:

يعد البريد الالكتروني من الخدمات المهمة التي تقدمها شبكة المعلومات الدولية الإنترنت، وهو شكل من أشكال الاتصال الإلكتروني يسمح لمستخدمي الإنترنت في نقل الرسائل بدلًا من الوسائل التقليدية، مما

(308) Dreyfus D. The idiot savants. Guide to rubberhose. http://www.rubberhose.org

يعني أنه صندوق بريد خاص على شبكة "الإنترنت" تمامًا مثل صندوق البريد العادي، حيث يمكن من خلاله إرسال الرسائل الإلكترونية من وإلى أشخاص آخرين.

وبالنظر إلى سهولة استخدامه صار أكثر وسائل الإنترنت شيوعًا واستخدامًا في الوقت الحاضر، ونظرًا لصعوبة إيجاد رقابة مُحكمة عبر شبكة "الإنترنت" فإنه لا يوجد بالتبعية ضوابط تحكم هذا البريد، مما نتج عنه بعض الاستخدامات غير المشروعة للبريد الإلكتروني (309).

ومن المسائل المهمة فيما يرتبط بالبريد الإلكتروني ضرورة مراعاة سريته، وهو ما جعل مبتكري برامجه يقومون بابتكار برامج تشفير خاصة به بحيث لا يستطيع أحد رؤية أي رسالة إلا للشخص الذى يعرف هذه الشفرة، ويمكن وضع البريد الإلكتروني في صندوق بريد خاص أو في ملف، أو طباعة الرسالة والاحتفاظ بها، ولقد ساعد ظهور التوقيع الإلكتروني في تسهيل عملية المراسلة عبر البريد الإلكتروني، حيث يقوم البرنامج بتخزين توقيع المستخدم كرمز أو شفرة ويقوم بوضعه تلقائيًا على كل رسالة.

ولقد تغير اليوم مفهوم المستندات فقد حلت المستندات الرقمية محل كثير من الوثائق المطبوعة على الورق، وتعد الرسائل الإلكترونية بذلك مستندات، حيث أصبح مفهوم المستند الذي يتفق مع ثورة الاتصالات عن بُعد وكل أسلوب تحدد به فكرة معينة أو تعبير محدد عن طريق كتابة ورقة أو كتابة إلكترونية، حيث إن العالم يعيش حاليًا عصر الثورة الرقمية، فقد أصبحت الكلمة والصوت والأشعة والصورة والمعلومات رقمية، حتى يمكن القول أصبحت للأرقام اليد العليا.

وتم الاعتراف للمستندات الإلكترونية بحجيتها في الإثبات في الكثير من التشريعات وأنها يجوز أن تكون مجال يقع عليه التزوير – مثلًا – فإذا كان محتوى المحرر قد أصبح يعبر عنه بلغة رقمية، فإن هذه اللغة هي التي حلت محل الكتابة، ومن ثم فإن هذا المحرر الرقمي يصلح لتقع عليه جريمة التزوير، فالمستند الإلكتروني مادام عبر عن فكرة وكان من الممكن قراءته وفهم معناه وإدراك مضمونه فإنه يعد

(309) إبراهيم. خالد ممدوح. (2008). *أمن الجريمة المعلوماتية*. مصر: الدار الجامعية للطباعة والنشر. ص 90.

محررًا، ومن ثم فإنه يحوز الحجية بحسب طبيعة الشخص الذي ينسب إليه إصداره ولمن وضع عليه توقيعه الإلكتروني.

ومن الجدير بالذكر أنه بصدور القانون الفرنسي الجديد سنة 1994م، فقد تم إلغاء المادتين رقمى 5/462 و6/46 واللتين نص عليهما القانون رقم 88/19 الصادر في 1988/1/5، بخصوص تجريم الغش الإلكتروني، وكانت المادة الأولى تنص على تجريم تزوير المستندات المعالجة آليًا، في حين كانت الأخرى تجرم استخدام هذه المستندات المزورة، وقد حلت محلهما المادة 441 من الكتاب الرابع من قانون العقوبات، بحيث أضيف إليها تزوير المستندات المعالجة آليًا واستعمالها، وقد أصبح نص هذه المادة بعد تعديلها تنص على أنه: "يعد تزويرًا "كل تغيير بطريق الغش للحقيقة في مكتوب أو في أي دعامة أخرى تحتوي على تعبير عن الفكر"، وهكذا حدث تطور في جريمة التزوير في الجرائم الإلكترونية من مجرد جريمة تزوير المستندات المعالجة آليًا فقط واستعمالها إلى جريمة تزوير المستندات الإلكترونية واستعمالها.

وبما أن الرسائل الإلكترونية التي تصل بواسطة البريد الإلكتروني تعد بمثابة رسائل شخصية فإنه يلزم حمايتها بالحماية ذاتها التي تتمتع بها الرسائل الورقية، ومن ثم فلا يجوز التنصت عليها أو الاطلاع على الأسرار التي تحتويها إلا بالطرق ذاتها التي تنص عليها قوانين الإجراءات الجنائية[310].

حيث إنه لا يستطيع المحقق اختراق صندوق البريد الإلكتروني أو الدخول على أنظمة الحاسب الآلي المحفوظ به رسائل البريد الإلكتروني وضبطها إلا بعد إتباع الإجراءات المنصوص عليها في القوانين الإجرائية والتي تنظم ذلك.

(310) حمودة. علي محمود علي. (2003) "الأدلة المتحصلة من الوسائل الإلكترونية. في إطار نظرية الإثبات الجنائي". ***بحث بالمؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية***. الامارات: أكاديمية شرطة دبي. الفترة من 26-4 إلي 28-4-2003. ص8.

ب– بيانات تنشر على مواقع التواصل الاجتماعي:

وهذه المواقع كثيرة، منها على سبيل المثال Facebook، وTwitter وInstagram وهذه المواقع تتيح لمستخدمها وضع الملفات بكافة أنواعها، سواء صور أو فيديو أو مستندات ويسمح بانتشارها على الشبكة، بحيث يستطيع أي مشترك في الموقع أن يقوم بتحميلها أو يعيد نشرها مرة أخرى، وهي بهذه الميزة تعد أخطر أنواع البيانات المتحركة على الإطلاق إذ أنها تسمح لأي شخص أن يكون وسيلة إعلامية منفردة قد تصل لكافة بقاع الأرض في عدة دقائق، وقد يقوم البعض باستغلال هذه الوسيلة استغلالًا خاطئًا فيعمل على نشر الشائعات، وهدم القيم، والترويج للفتن، والتحريض على الرذيلة بدون رقيب عليه أو رادع إلا نفسه.

وقد شهدت الفترة الأخيرة في الوطن العربي المثال الحي على خطورة الاستغلال السيئ لهذه المواقع، وما أدى إليها من انهيار لبعض الدول بسبب بعض الأخبار الكاذبة التي انتشرت على كافة المستويات.

ج – بيانات تبث عبر مواقع مخصصة لبث الأفلام المصورة:

وهو نوع من المواقع يتيح للمستخدم حفظ ملفاته المصورة على الموقع ليراها من يريد أن يطلع عليها، وأشهر هذه المواقع هو YouTube، وهو موقع يتيح لك أن تنشر أفلامك المصورة على الموقع ليراها كل شخص في العالم يستطيع الدخول على الإنترنت، وهو أيضًا موقع شديد الخطورة، إذ أنه يسمح للمجرمين أن يقوموا بنشر أفلام فيديو ملفقة وغير حقيقية يخدع بها البسطاء وقليلي الخبرة الذين لا يقدروا على كشف تزييفها، أو يقوم بعض ضعاف النفوس بتصوير أفلام خلسة لبعض الناس ويقوموا بابتزازهم وتهديدهم بالنشر على تلك المواقع.

وأيضًا هناك برنامج Bambuser وهو برنامج يتيح للمستخدم تصوير الأحداث مباشرة ورفعها للموقع الذي يحمل نفس الاسم Bambuser عن طريق أي هاتف به تقنية 3G – الخاصة بالهواتف المحمولة – فيسمح لكافة المشتركين في الموقع برؤيتها في زمن تأخير لا يتعدى دقيقة واحدة.

وهذا البرنامج هو ما تقوم به بعض القنوات الإخبارية، والممنوعة من العمل داخل بعض الدول باستغلاله عن طريق بعض ضعاف النفوس فيقوموا بدور بديل لمراسلين القناة الممنوعين من ممارسة عملهم في هذه الدول نظرًا لتوجهاتهم المعادية للدولة.

د- بيانات محفوظة على الشبكة:

وهذا النوع أشبه بخزائن البنوك السرية التي يتم حفظ الأشياء الثمينة بها ولا يتم فتحها إلا بمعرفة أصحابها، أو من يعلمون الشفرة الخاصة بفتحها، فهي مواقع خصصت لحفظ المستندات الهامة على الشبكة لحفظها من الإتلاف أو الضياع، ولا يتم الاطلاع عليها إلا لمن يملك كلمة المرور الخاصة بها إلا لو سمح مالك الملفات نفسه بنشرها للكافة وسمح لأي شخص بالاطلاع عليها دون كلمة مرور.

خلاصة الفصل

الدليل الجنائي إذا هو الأداة الواقعية التي يقصد منها توجيه القاضي الجنائي بأن الفعل الإجرامي قام به المتهم، ويقع به الإثبات، وعلى ذلك فالدليل الجنائي كل أداة مرخص بها قانونًا لإثبات وجود الواقعة المرتكبة أو عدم وجودها أو صحة أو كذب وقوعها. أي أنه الدليل المطلوب للتثبت من الفعل الجنائي لكي يكون هناك فصل في الدعوى الجنائية بالبراءة والإدانة. فالدليل هو مقوم حكم القاضي وله تقدير أهميته وملاءمته، كما أنه يمكن استخلاص من التعريفات التي وردت في هذا الشأن أن الدليل الجنائي هو التي تستعين بها أجهزة العدالة في كشف الحقيقة، عن طريق تأكيد الاتهام أو نفيه. وبناء على ذلك قام الباحث بتقسيم هذا الفصل إلى ثلاثة مباحث، استعرض في الأول مفهوم الدليل الرقمي وخصوصية جريمة نشر الأخبار الكاذبة عبر وسائل التواصل الاجتماعي، من حيث تقسيم هذا المبحث إلى عدة مطالب عرض من خلالها لمفهوم الدليل الرقمي، وخصوصية جريمة نشر الأخبار الكاذبة عبر وسائل التواصل الاجتماعي من حيث تميز تلك الجريمة عن باقي الجرائم بصفات تميزها وتجعلها متفردة عنهم، واختتم هذا المبحث باستعراض أحكام الأدلة الرقمية التي يمكن تحصيلها من جريمة نشر الأخبار الكاذبة عبر وسائل التواصل الاجتماعي. كما انتقل الباحث في دراسة هذا الفصل إلى عرض لإشكاليات مكافحة جريمة نشر الأخبار الكاذبة عبر وسائل التواصل الاجتماعي وما تتطلب عرض خصائص الدليل الرقمي والصعوبات التي يمكن أن تواجه رجال الضبط في الحصول على هذا الدليل، وباعتبار تلك الجريمة عابرة للحدود والقارات فقد وجدت مشكلة الاختصاص، وكيف يمكن التغلب عليها وفق القانون الاتحادي الإماراتي. واختتم الباحث هذا الفصل بعرض الإشكاليات المتعلقة بضبط المجرمين في جريمة نشر الأخبار الكاذبة عبر وسائل التواصل الاجتماعي من حيث إجراءات التفتيش الخاصة بتلك الجريمة، والمعاينة الإلكترونية للوسط المحيط بتلك الجريمة من حيث طبيعة البيانات الرقمية نفسها التي يمكن مسحها أو تغييرها بسهولة لذلك من الضروري جمعها والاحتفاظ بها بسرعة كلما أمكن، وإذا كان المرور بالشبكات لا يستغرق إلا جزءًا من الثانية وهي فترة قصيرة جدًا ونظرًا لحجم الملفات الكبيرة وهو ما يعد صعوبة كبيرة، وهو ما ينقلنا إلى وجود إشكالية تتعلق بإثبات جريمة نشر الأخبار الكاذبة عبر وسائل التواصل الاجتماعي لأن الوسط الذي تتحرك وتنشأ فيه الجريمة متغير ويوجد من الصعوبات الكثيرة في إثباته، وقد استعرض الباحث هذا الموقف القانوني سواء الوطني أو الدولي.