**جامعة عباس لغرور خنشلة**

**الملتقى الدولي الافتراضي حول**

**" العنف والتطرف والإرهاب بأبعاده الدينية والسياسية والاجتماعية "**

**اللقب والاسم**: هارون نورة
**الوظيفة والرتبة العلمية**: أستاذة محاضرة صنف " أ "
**المؤسسة المستخدمة:** كلية الحقوق والعلوم السياسية جامعة بجاية
**المخبر:** مخبر البحث حول فعلية القاعدة القانونية
**رقم الهاتف:** 0797507993
**البريد الالكتروني:** nora06dz2016@yahoo.com

**اللقب والاسم:** بن بوعبد الله نورة
**الوظيفة والرتبة العلمية**: أستاذة محاضرة صنف " أ "
**المؤسسة المستخدمة:** كلية الحقوق والعلوم السياسية جامعة باتنة 1
**رقم الهاتف:** 0542350078
**البريد الالكتروني:** norabenbouabdallah@gmail.com
**المحور:** السادس " مساعي الدول الإسلامية والدولية في مكافحة الإرهاب والعنف والتطرف ".
**عنوان المداخلة:**

# اعتماد الوسائل الالكترونية الحديثة في مكافحة جرائم الإرهاب الرقمي

# Adopt modern electronic means in the fight against digital terrorism crimes

**الملخص:**

أصبح الإرهاب الالكتروني يشكل خطرا حقيقيا يهدد العالم بأسره، إذ أن اعتماد الإرهابيين على التطور التكنولوجي وشبكات الاتصال مكنهم من تنفيذ العمليات الإرهـــــــابية الالكترونية من أي مكـــان يتواجدون فيه وبكل سهولة، من هنا وجب مواكبة هذا التطور وخلق وسائل تقنية حديثة كفيلة بمكافحة هذا الإجرام الخطير، وهو ما قام به المشرع الجزائري بموجب القانون رقم 06-22 المعدل والمتمم لقانون الإجراءات الجزائية، والقانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها؛ من هنا تسعى هذه الدراسة إلى إبراز الوسائل التقنية المعتمدة من طرف المشرع لمكافحة الإرهاب الالكتروني من جهة، والتطرق لحجية الدليل المتحصل عليه من خلال هذه الترتيبات التقنية في إدانة الإرهابيين من جهة أخرى.

**الكلمات المفتاحية:** الإرهاب الالكتروني، المراقبة الالكترونية، تفتيش المنظومات المعلوماتية، الدليل الالكتروني.

**Abstract:**

Electronic terrorism has become a threat to the whole world, For terrorists' dependence on technological development and communication networks has enabled them to conduct electronic terrorist operations wherever they are and with ease. It is therefore necessary to follow this evolution and to create modern technical means to fight against this serious crime, which the Algerian legislator has done in accordance

with the law n ° 06-22 of December 20, 2006 modifying and supplementing the code of criminal procedure, and Law no. 09-04 of 5 August 2009 laying down specific rules relating to the prevention and fight against offenses related to information and communication technologies; this study seeks to highlight the technical means adopted by the legislator to fight against electronic terrorism on the one hand, and to address the probative value of the evidence obtained thanks to these technical devices to convict terrorists on the other hand.

**Keywords:** Electronic terrorism, Electronic surveillance, Computer systems search, digital evidence.

**مقدمة:**

أدى التقدم التكنولوجي إلى ظهور صور جديدة من الإجرام تعرف بالإجرام المعلوماتي، ولعل أخطرها الإرهاب الإلكتروني[1] الذي تختلف أسبابه ( شخصية[2]، فكرية[3]،...)، والأهم من ذلك أنه يعتمد في نشاطه على استخدام التقنية الإلكترونية الرقمية، كوسيلة لتنفيذ الفعل الإجرامي المستهدف، فالإرهاب الالكتروني أو ما يعرف بالإرهاب الرقمي أو المعلوماتي أو السبراني، يتميز باعتماده على الوسائل الالكترونية، وتأثره بالتطور الحاصل في مجال التكنولوجيا وتنامي استخدام شبكة الانترنيت، التي جعلت من العالم مجرد قرية صغيرة لا تعرف الحدود الجغرافية، ما جعل هذا النوع من الإجرام الخطير يشكل تهديدا أمنيا وعصريا للمجتمع الدولي بأسره فهو من الجرائم المنظمة[4] العابرة للحدود الوطنية التي تمتد آثارها ومخاطرها( السياسية، الاجتماعية، الاقتصادية،...) إلى كافة الدول، فهو أصبح الأسلوب والخيار الأسهل للجماعات الإرهابية[5].

من أهم مظاهر الإرهاب الالكتروني نجد تبادل المعلومات الإرهابية ونشرها عبر شبكة المعلوماتية الدولية، حيث تسهل هذه الأخيرة على الإرهابيين نشر أفكارهم المتطرفة ونشر ثقافة الإرهاب والترويج لها عبر مختلف مواقع التواصل الاجتماعي[6] كالفيسبوك، التويتر، اليوتوب وغرف الحوار الالكترونية...، كما نجد أيضا من مظاهر الإرهاب الالكتروني إنشاء مواقع إرهابية إلكترونية لاسيما تلك المستهدفة للنظم العسكرية[7]، حيث تستغل الجماعات الإرهابية هذه المواقع لممارسة نشاطاتها المختلفة من دعاية ونشر للأفكار المتطرفة سواء كانت سياسية أو دينية أو عنصرية، وتجنيد الأشخاص لاسيما فئة الشباب في واستخدامهم إما بطريق الترغيب

---

[1]- يعرف الإرهاب الالكترونى بأنه " العدوان أو التخويف أو التهديد المادي أو المعنوي الصادر من الدول ، أو الجماعات أو الأفراد على الإنسان، باستخدام الموارد المعلوماتية والوسائل الإلكترونية، بشتى صنوف العدوان وصور الفساد " ، هشام بشير ، الإرهاب الإلكتروني في ظل الثورة التكنولوجية وتطبيقاتها في العالم العربي ،مجلة آفاق سياسية، المركز العربي للبحوث والدراسات، مصر، العدد 6 يونيو 2014 ، ص 77.

[2]- من أهم الأسباب الشخصية لانتشار الجرائم الإرهابية، نجد الرغبة في الشهرة أو الفشل في الحياة من كل جوانبها، ما يولد الشعور بعدم الانتماء للوطن والرغبة في الانتقام من خلال ولوج عالم الإجرام والإرهاب والانحراف، الهويدي عمر، مكافحة جرائم الإرهاب، دار وائل للنشر، عمان، 2011، ص. 54.

[3]- من أهم الأسباب الفكرية لانتشار الجرائم الإرهابية، نجد التطرف والتعصب الديني إلى جانب الجهل والأمية، مصطفى يوسف كافي، الإدارة الالكترونية، د. ط، دار رسلان للطباعة والنشر، سوريا، دمشق، 2011، ص. 439، أمين فرج، الجريمة الالكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والانترنيت، ط. 1، مكتبة الوفاء القانونية، الإسكندرية، 2011، ص. 224.

[4]- تتشابه الجريمة المنظمة مع الإرهاب من حيث طبيعة العمل الذي يعرف بالتنظيم والتخطيط، والتنفيذ بشكل دقيق وسري، ونشر الرعب والخوف والرهبة في نفوس الأشخاص والدولة في آن واحد، يوسف حسن يوسف، الجريمة المنظمة الدولية والإرهاب الدولي، المصدر القومي للإصدارات القانونية، ط.1، القاهرة، 2010، ص. 55.

[5]- عبد الله عبد العزيز بن فهد العجلات، الإرهاب الالكتروني في عصر المعلومات، بحث مقدم إلى المؤتمر الدولي الأول حول " حماية أمن المعلومات والخصوصية في قانون الانترنيت المنعقد في القاهرة، مصر، يوم 2 إلى 4 يونيو، 2008، ص. 12.

[6] تعرف شبكات التواصل الاجتماعي بأنها " شبكات تفاعلية تتيح لمستخدميها التواصل فى أى وقت وفى أى مكان فى العالم "، نورا بندارى عبد الحميد فايد، دور وسائل التواصل الاجتماعي في تجنيد أعضاء التنظيمات الإرهابية، دراسة حالة " داعش " متوفر على الرابط: https://democraticac.de/?p=34268، تم الاطلاع عليه بتاريخ 7/4/ 2021.

[7]- حيث تتسلل الجماعة الإرهابية إلكترونيا إلى الأنظمة الأمنية في الدولة وتقوم بتعطيل مراكز القيادة العسكرية ومختلف وسائل الاتصال للجيوش وهذا بدافع توجيهها إلى أماكن غير آمنة بهدف تفجيرها، أسعد طارش عبد الرضا، علي إبراهيم مشجل المعموري، الأمن السبراني ودوره في انتشار ظاهرة الإرهاب في العراق بعد العام 2003، مجلة دراسات دولية، العدد 80، ص. 169، متوفر على الرابط: https://www.iasj.net/iasj/download/5e08943c7ae82efb، تم الإطلاع عليه بتاريخ 7/ 4/ 2021.

أو الترهيب للانضمام إلى العناصر والجماعات الإجرامية المحلية والدولية وإعدادهم مادياً ومعنوياً للعمل فى خدمة هذه العناصر والجماعات[8].

فالوسائل التقنية والعلمية تجعل من تنفيذ العمليات الإرهابية أكثر دقة وسهولة، وهذا راجع لسهولة الاتصال بعناصر الجماعة الإرهابية من خلال استعمال الرسائل المشفرة أين لا يكون الإرهابي مضطرا للإفصاح عن هويته الحقيقة، فهي تقنية علمية لا تترك أثرا يدل عليها[9]؛ كما تسهل هذه الشبكة العنكبوتية عملية تمويل الجماعات الإرهابية ( شراء الأسلحة ومختلف المعدات اللازمة لتنفيذ العملية الإرهابية)، وذلك من خلال اللجوء إلى عمليات غسيل الأموال، التي تقوم بها المنظمات الإرهابية بالتعاون مع المصارف عبر الانترنيت، أو عن طريق تزوير بطاقات الائتمان أو استغلال الجمعيات الخيرية[10].

أصبح الفضاء الإلكتروني عاملا مساعدا ووسيطا في تنفيذ العمل الإرهابي[11]، الأمر الذي جعل مكافحة الإرهاب الالكتروني وإثباته صعبا في ظل وسائل الإثبات التقليدية، التي لم تعد تكفي لمواكبة هذا التطور التقني، مما جعل اللجوء لاستغلال التكنولوجيا، والوسائل التقنية الحديثة أمرا محتوما لمكافحة هذا النمط من الإجرام، وإقامة الدليل على وقوعها ومعاقبة المتورطين في ارتكابها، وهو ما تسعى إلى توضيحه هذه الدراسة من خلال الإجابة على تساؤل جوهري يكمن في **ماهية الوسائل التقنية المعتمدة في القانون الجزائري لمكافحة الإرهاب الالكتروني، وما مدى حجية الدليل المتحصل عليه في إدانة المتورطين في ارتكاب هذا النمط الخطير من الإجرام ؟**

تقتضي الإجابة على هذه الإشكالية اعتماد المنهج التحليلي الوصفي، وذلك من خلال تحليل النصوص القانونية المرتبطة بالموضوع، معتمدين في ذلك على التقسيم الثنائي، حيث نتطرق أولا لتحديد أهم وسائل التكنولوجيا الحديثة المعتمدة في القانون الجزائري لمكافحة الإرهاب الالكتروني**(المحور الأول)**، ثم التطرق لمسألة في غاية الأهمية تتمثل في القيمة القانونية للدليل الإلكتروني في مجال إثبات جرائم الإرهاب الرقمي**(المحور الثاني).**

## المحور الأول

## أهم الوسائل الالكترونية الحديثة المعتمدة لمكافحة جرائم الإرهاب الرقمي

أدركت التشريعات المختلفة للدول، بمحدودية الأساليب التقليدية الكلاسيكية في مكافحة الجرائم الإرهابية، لاسيما تلك التي تعتمد على التقنيات الحديثة، ما دفعها لمواكبة التطور التكنولوجي واعتماد الوسائل التقنية لمكافحة هذا النمط الخطير من الإجرام وذلك بمطابقة تشريعاتها مع هذه المتطلبات الحديثة[12].

يعد التشريع الجزائري واحدا من بين هذه التشريعات، التي أدركت عجز أساليب البحث والتحري التقليدية لمكافحة الإرهاب الالكتروني، ما جعله يعتمد على الوسائل التقنية الحديثة لمكافحة هذا الإجرام الخطير حيث استحدث– بعد مصادقته على اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية[13]- ما يعرف بالترصد الالكتروني لإثبات الجرائم الخطيرة بما فيها جرائم الإرهاب، وذلك بموجب القانون رقم 06-22 المعدل والمتمم لقانون الإجراءات الجزائية[14]، كما أكد على أهمية هذه التقنية لاحقا بموجب القانون رقم 09-04 المتضمن

---

[8]- حصة عبد الله بن سليمان ، دور مجلس التعاون الخليجى فى مكافحة الاتجار بالبشر ، رسالة دكتوراه، كلية الاقتصاد والعلوم السياسية ، القاهرة، 2013، ص. 20.

[9]- حسنين شفيق، الإعلام الجديد والجريمة الالكترونية، التسريبات، التجسس الالكتروني، الإرهاب، دار فكر وفن، مصر، 2014، ص. 292.

[10]- أسعد طارش عبد الرضا، علي إبراهيم مشجل المعموري، مرجع سابق.

[11]- نورا بندارى عبد الحميد فايد، مرجع سابق.

[12] -Nouvelles méthodes de lutte contre la criminalité, la normalisation de l'exception, étude de droit comparé: Belgique, Etats-Unis, Italie, Pays-Bas, Allemagne, sous la direction de Maria Luisa Cesoni, Bruylant , LGDJ, 2007, p. 57.

[13]- اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، اعتمدت وعرضت للتوقيع والتصديق والانضمام بموجب قرار الجمعية العامة للأمم المتحدة، المؤرخ في 15 نوفمبر2000، صادقت عليها الجزائر بموجب مرسوم رئاسي رقم 02- 55، مؤرخ في 5 فبراير 2002، ج. ر. عدد 9، مؤرخة في 10 فيفري 2002.

[14]- قانون رقم 06-22، مؤرخ في 20 ديسمبر 2006، يعدل ويتمم أمر رقم 66 – 155، مؤرخ في 8 يونيو 1966، يتضمن قانون الإجراءات الجزائية، ج. ر عدد 84، مؤرخة في 24 ديسمبر 2006.

القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[15]، حيث سمح باللجوء إلى المراقبة الالكترونية في مجال البحث والتحري والتحقيق عن جرائم الإرهاب**(أولا)**، كما سمح أيضا باعتماد أسلوب تفتيش النظم المعلوماتية، أو ما يعرف بالتفتيش المعلوماتي**(ثانيا)**.

**أولا- المراقبة الإلكترونية:**

سمح المشرع بموجب القـــــــانون رقم 06-22 المعدل والمتمم لقانون الإجراءات الجزائية، وكذا القـــــــانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيـــــات الإعلام والاتصال ومكافحته، بالمساس بالحق في حرمة الحياة الخاصة، إذ أباح بموجب المادة 65 مكرر 5 من القانون الأول باعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية، وكذا وضع الترتيبات التقنية دون موافقة المعنيين، من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية أو التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص.

كما أباح ذلك أيضا بموجب المادة 3 من القانون رقم 09-04 التي جاء مضمونها كما يلي " مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات، يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية، وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون، وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية[16] وتجميع وتسجيل محتواها في حينها..."؛ يسمح المشرع بإجراء مثل هذا الترتيب التقني للوقاية من جرائم الإرهاب وهذا ما يفهم من نص المادة 4/أ من القانون رقم 09-04 التي ورد مضمونها تحت عنوان " الحالات التي تسمح باللجوء إلى المراقبة الالكترونية " كمـــــا يلي" يمكن القيام بعمليات المراقبة[17]المنصوص عليها في المادة 3 أعلاه في الحالات الآتية: أ- للوقاية من الأفعـــــال الموصوفة بجرائم الإرهـــــاب أو التخريب أو الجرائم الماسة بأمن الدولة "[18].

بالنظر لخطورة هذه الترتيبات التقنية على حرمة الحياة الشخصية للأفراد، جعل المشرع أمر اللجوء لاستعمال هذه الترتيبات مرهونا بضرورة توافر ضوابط معينة أهمها الحصول على إذن من الجهة القضائية المختصة، وقد حرص المشرع على هذا الضابط بالنص عليه في القانون رقم 06-22 المعدل والمتمم لقانون الإجراءات الجزائية[19]، وكذا القانون رقم 09-04 الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[20].

الاختلاف الموجود بين أحكام المراقبة الالكترونية في كلا القانونين هو أن القانون رقم 06-22 يسمح باللجوء لهذا الأسلوب التقني في حالة وقوع الجريمة الإرهابية، واقتضت ضرورات التحري أو التحقيق الابتدائي اللجوء لهذا الأسلوب، أي أنه لا يمكن اللجوء لهذا الإجراء الاستثنائي في حال عدم وقوع الجريمة، في حين يسمح بذلك القانون رقم 09-04 حيث يهدف المشرع من وراء أسلوب مراقبة الاتصالات الإلكترونية حسب المادة 4 من هذا القانون إلى الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن

---

[15]- قانون رقم 09-04، مؤرخ في 5 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتهما، ج. ر عدد 47، مؤرخة في 16 أوت 2009.

[16]- " يقصد بالاتصالات الالكترونية أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية "، المادة 1/و من قانون رقم 09-04، مؤرخ في 5 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتهما، المرجع نفسه.

[17] - يفيد مصطلح " مراقبة " الذي استعمله المشرع في القانون رقم 09-04 نفس مصطلح " اعتراض " الذي استعمله في القانون رقم 06-22.

[18]- كما يجيز المشرع اللجوء لأسلوب مراقبة الاتصالات الالكترونية في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني، كما يجيز ذلك أيضا لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الالكترونية ، وأيضا في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة، المادة 4 من قانون رقم 09-04، مؤرخ في 5 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، مرجع سابق.

[19]- المواد 65 مكرر 5 إلى 65 مكرر 7 من أمر رقم 06-22، مؤرخ في 20 ديسمبر 2006، يعدل ويتمم أمر رقم 66-155، مؤرخ في 8 يونيو 1966، يتضمن قانون الإجراءات الجزائية، مرجع سابق.

[20]- المادة 4 من قانون رقم 09-04، مؤرخ في 5 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، مرجع سابق.

الدولة، وهذا لكون القانون رقم 09-04 قد تم سنه أساسا من أجل وضع قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتهما[21]؛ ولكن هذا لا يمنع من اللجوء لاستعمال هذا الأسلوب التقني بعد وقوع الجريمة لغرض البحث والتحقيق في هذه الجرائم، وفقا لأحكام الفقرة ج من المـــــادة 4 من هذا القانون.

ما يجعلنا نفهم أن المشرع قد اعتمد المعيار الزمني الموسع لاستعمال أسلوب المراقبة الالكترونية، ومع أن الحكمة من وراء هذا التوسيع هو الكشف المبكر عن جرائم الإرهاب وإجهاض المخطط الإجرامي للإرهابيين، إلا أن هذا التوسع يطعن من جهة أخرى في الحق في حرمة الحياة الخاصة للأفراد باعتباره حقا دستوريا وقانونيا.

**ثانيا- تفتيش المنظومات المعلوماتية ( التفتيش المعلوماتي ):**

التفتيش هو إجراء من إجراءات التحقيق، ووظيفته البحث عن أدلة الجريمة، فهو ليس دليلا بذاته بل هو وسيلة للحصول على الدليل[22]؛ ومع تطور أساليب ارتكاب الجريمة واعتماد الجناة على التطور التكنولوجي لتنفيذ سلوكهم الإجرامي، ظهر نوعا آخر من التفتيش مرتبطا بالحاسوب وشبكة الانترنيت، وهو ما يعرف بالتفتيش المعلوماتي[23] أو ما عبر عنه المشرع في القانون رقم 09-04 بـ " تفتيش المنظومات المعلوماتية "، ويعرف الفقه هذا الإجراء التقني بأنه البحث في مستودع سر المتهم عن أشياء مادية أو معنوية، تفيد في كشف الحقيقة ونسبتها إليه، فالتفتيش المعلوماتي هو عبـــــارة عن بحث واطلاع دقيق على محل منحه القـــــانون حماية خاصة، باعتباره مستودع سر صاحبه سواء كان حاسوبا أو أنظمة أو إنترنيت[24]، أو هاتفا أو آلة تصوير رقمية أو بطاقة ذاكرة...

نظم المشرع الجزائري إجراء تفتيش المنظومات المعلوماتية بموجب المواد من 5 إلى 9 من القانون رقم 09-04 الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصـــال ومكافحتها، ولم يتطرق المشرع لتعريف هذا الأسلوب التقني، واكتفى فقط بتعريف المنظومات المعلومـــــاتية بأنها" أي نظلم منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين "[25].

إذا تبين مسبقا بأن المعطيـــــات المبحوث عنهـــا، والتي يمكن الدخـــول إليها انطلاقا من المنظومة الأولى، مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة، طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل[26]، لذا يسمح المشرع باللجوء إلى تفتيش المنظومات المعلوماتية في إطار تنفيذ طلبات المساعدة القضائية المتبادلة[27].

إن إجراء التفتيش - بوصفه من إجراءات التحقيق – عادة ما يكون عند وقوع الجريمة، ولا يجوز إجراؤه من أجل جريمة محتملة الوقوع ولو كانت هناك مؤشرات على جدية احتمال وقوعها[28]، غير أن المشرع

---

[21]- المادة الأولى من قانون رقم 09-04، مؤرخ في 5 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، المرجع نفسه.

[22]- رضا هميسي، " تفتيش المنظومات المعلوماتية في القانون الجزائري "، مجلة العلوم القانونية والسياسية، جامعة الوادي، عدد 5، جوان 2012، ص. 159.

[23]- يجب أن يكون القائم بالتفتيش المعلوماتي متخصصا في التحقيق الجنائي ومعالجة البيانات، لأن هذا النوع من التفتيش يتعلق بالفضاء الافتراضي وأوعية التخزين وتفتيش للبيانات التي يحفظها جهاز الحاسوب، عبد الله بن عبد العزيز بن عبد الله الخثعمي، التفتيش في الجرائم المعلوماتية، دراسة تطبيقية، رسالة ماجستير في العدالة الجنائية، جامعة نايف العربية للعلوم الأمنية، الرياض، 2011، ص. 35.

[24]- علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنيت، دراسة مقارنة، ط. 1، عالم الكتاب الحديث للنشر والتوزيع، إربد، 2004، ص. ص. 12، 13.

[25]- المادة 2/ب من قانون رقم 09-04، مؤرخ في 5 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، مرجع سابق.

[26]- المادة 5 من قانون رقم 09-04، مؤرخ في 5 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، المرجع نفسه.

[27]- المادة 4 من قانون رقم 09-04، مؤرخ في 5 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، المرجع نفسه.

[28]- علي حسن محمد الطوالبة، مرجع سابق، ص. 62.

الجزائري بموجب القانون رقم 09-04 قد أجاز اللجوء لإجراء تفتيش المنظومات المعلوماتية **للوقاية** من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، كما أجاز اللجوء لهذا الأسلوب التقني في حال توفر معلومات عن مجرد **احتمال** اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني، وتفيد عبارتي " الوقاية " و" احتمال " التي استعملها المشرع في المادتين 1 و 4 من القانون رقم 09-04 أن الجريمة لم تقع بعد، ما يعني إمكانية اللجوء لإجراء التفتيش المعلوماتي كتدبير وقائي سابق لوقوع الجريمة، وهو ما يطعن في الحق في حرمة الحياة الخاصة لصاحب الأنظمة المعلوماتية وحرمة أسراره، فتفتيش الأنظمة المعلوماتية يهدد الحياة الخاصة للأفراد ومن خلالها يمكن جمع كم هائل من المعلومات عن الحياة الخاصة للأفراد[29]؛ خاصة وأن جمع المعلومات والبحث عنها يتم دون علم أو رضا صاحب الأنظمة المعلوماتية[30].

في حال ما إذا اكتشفت السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية، وفي كل الأحوال يجب على السلطة المختصة بالتفتيش والحجز أن تسهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية[31].

كما يمكن تصور عملية الحجز عن طريق منع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية، وهذا في الحالة التي يستحيل فيها إجراء الحجز وفقا للمادة 6 من القانون رقم 09-04، وذلك لأسباب تقنية[32]، وفي كل الأحوال لا يجوز – تحت طائلة العقوبات المعمول بها في التشريع المعمول- استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة المنصوص عليها في القانون رقم 09-04، إلا في الحدود الضرورية للتحريات أو التحقيقات القضائية[33].

---

[29] - Valérie-Laure BENABOU, Vie privé sur interne : Le traçage électronique, in les liberté individuelles à l'épreuve de NTIC, Etudes réunies sous la direction de Marie- Christine Piatti, PUL, 2001, p. p. 89-91.

[30]- عبد العزيز نويري، " المخاطر القانونية للانترنيت على حرية التعبير والحياة الخاصة "، مجلة التواصل، جامعة عنابة، عدد 26، جوان 2010، ص. 70.

[31]- المادة 6 من قانون رقم 09-04، مؤرخ في 5 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، مرجع سابق.

[32]- المادة 7 من قانون رقم 09-04، مؤرخ في 5 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، المرجع نفسه.

[33]- المادة 8 من قانون رقم 09-04، مؤرخ في 5 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، المرجع نفسه.

## المحور الثاني

## القيمة القانونية للدليل الإلكتروني في مجال إثبات جرائم الإرهاب الرقمي

إن اعتماد الوسائل الالكترونية لإثبات الجريمة المعلوماتية كجريمة الإرهاب الرقمي، يؤدي إلى طرح تساؤل حول مدى حجية الدليل الرقمي في إثبات الجريمة الالكترونية كالجريمة محل الدراسة؟

لم يتطرق المشرع لتعريف الدليل الرقمي، وذلك سواء في المادة الثانية من القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ولا في المادة 5 من المرسوم الرئاسي رقم 15-261، المحدد لتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[34].

تصدى الفقه لتعريف الدليل الرقمي على أنه " الدليل المأخوذ من أجهزة الكمبيوتر ويكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية، يمكن تجميعها أو وتحليلها باستخدام برامج تطبيقات وتكنولوجيا خاصة، وهي مكون رقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأصوات أو الأشكال أو الرسوم وذلك من أجل اعتماده أمام أجهزة إنفاذ وتطبيق القانون"[35].

ما يلاحظ على التعريف، أنه يحصر مفهوم الدليل الرقمي على ذلك المستمد من جهاز الكمبيوتر فقط، مع أن الحقيقة أن الدليل الرقمي يتسع ليطال كل ما يستمد من أي جهاز تقني آخر غير الحاسوب، كالهاتف وآلة التصوير وغيرها من الأجهزة التي تعتمد على التقنية الرقمية الحديثة.

لم يضع المشرع نصوصا قانونية تتعلق بكيفية قبول الدليل الرقمي في إثبات الجريمة، مما يجعلنا نعود لتطبيق القواعد العامة في قانون الإجراءات الجزائية، المطبقة على مسألة قبول الدليل الجنائي بصورة عامة، والتي تقضي بخضوع الدليل لمبدأ حرية القاضي الجنائي في الاقتناع، ومن جهة أخرى إخضاع هذه الحرية لضوابط معينة ،ما يجعلها حرية نسبية وغير مطلقة، من هنا يمكن القول أن الدليل الالكتروني يخضع لمبدأ حرية القاضي الجنائي في الاقتناع **(أولا)** مع خضوع هذا الأخير لضوابط محددة تعكس تقييد حرية القاضي الجنائي في هذا المجال**(ثانيا).**

**أولا- خضوع الدليل الرقمي لمبدأ حرية القاضي الجنائي في الاقتناع:** يعتبر مبدأ حرية القاضي الجنائي من أهم المبادئ التي يقوم عليها الإثبات في المسائل الجزائية، ويقضي هذا المبدأ بحرية القاضي الجنائي في قبول جميع الأدلة المقدمة إليه من قبل أطراف الدعوى وتقديرها بكل حرية، بما فيها الأدلة الرقمية كالدليل المستمد من التفتيش المعلوماتي أو المراقبة الالكترونية، فلا وجود لأدلة يحظر على القاضي الجنائي قبولها.

تبنى المشرع مبدأ حرية القاضي الجنائي في الاقتناع بالدليل في الفقرة الأولى من المادة 212 من قانون الإجراءات الجزائية[36] كما يلي" يجوز إثبات الجرائم بأي طريق من طرق الإثبات ما عدا الأحوال التي ينص فيها القانون على غير ذلك، وللقاضي أن يصدر حكمه تبعا لاقتناعه الخاص "؛ وأيضا المادة 307 من القانون ذاته، التي تقضي بحرية القضاة في بناء حكمهم على الاقتناع الشخصي كما يلي " إن القانون لا يطلب من القضاة أن يقدموا حسابا عن الوسائل التي بها قد وصلوا إلى تكوين اقتناعهم، ولا يرسم لهم قواعد بها يتعين عليهم أن يخضعوا لها على الأخص تقدير تمام أو كفاية دليل ما، ولكنه يأمرهم أن يسألوا أنفسهم في صمت وتدبر، وأن يبحثوا بإخلاص ضمائرهم في أي تأثير قد أحدثته في إدراكهم الأدلة المسندة إلى المتهم وأوجه

---

[34]- مرسوم رئاسي رقم 15-261، مؤرخ في 8 أكتوبر 2015، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج. ر عدد 58، مؤرخة في 8 أكتوبر 2015.

[35]- خالد ممدوح إبراهيم، الدليل الإلكتروني في الجرائم المعلوماتي، مقال منشور على الرابط: https://kenanaonline.com/users/KhaledMamdouh/posts/77859، تم الإطلاع عليه بتاريخ، 7/ 4/ 2021.

[36] - أمر رقم 66- 155، مؤرخ في 8 يونيو 1966، يتضمن قانون الإجراءات الجزائية، ج. ر عدد 48 ، مؤرخة في 11 جوان 1966، معدل ومتمم.

الدفـــــــاع عنها ولم يضع لهم القانون سوى هذا السؤال الذي يتضمن كل نطاق واجباتهم: هل لديكم اقتناع شخصي؟ ".

يفهم من خلال هذين النصين أن الجرائم بمختلف أنواعها- بما فيها الجرائم المعلوماتية ومنها المرتبطة بالإرهاب الالكتروني- تخضع لمبدأ حرية الإثبات الذي يقوم على حرية القاضي الجنائي في قبول جميع الأدلة المطروحة أمامه، من قبل أطراف الدعوى بما فيها الأدلة الرقمية، ورغم عدم نص المشرع الجزائري على قبول الدليل الرقمي بموجب نصوص صريحة، إلا أنه اعتمد بموجب القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، على طرق حديثة لاستخلاص الدليل الرقمي كمراقبة الاتصالات الإلكترونية، تفتيش المنظومـــــات المعلوماتية، حجز المعطيات المعلوماتية، التي تفيد في الكشف عن الجرائم ومرتكبيها، وهذا ما يدفعنا للقول بأن المشرع الجزائري اعتمد قبول الأدلة الرقمية لإثبـــــات الجريمة المعلومـــــاتية دون تسميتها بشكل صريح، ولعل السبب في ذلك راجع لوجود نص المادتين 212 /1 و307 من قانون الإجراءات الجزائية أعلاه، ولكن حبذا لو كرس المشرع تبنيه للأدلة الرقمية بموجب نصوص صريحة، نظرا لخطورة الجريمة المعلوماتية لاسيما في مجال الجماعات والمنظمات الإرهابية، التي تمارس نشاطها في ظل الرقمنة.

**ثانيا- شروط قبول الدليل الرقمي لإثبات جريمة الإرهاب الالكتروني:** يقضي مبدأ حرية الاقتناع الشخصي للقاضي الجنائي، منحه سلطة واسعة في تكوين عقيدته من أي دليل يطرح أمامه، إلا أن هذه الحرية ليست مطلقة، وإنما تفرض عليها قيودا في شكل ضوابط يجب على القاضي الجنائي التقيد بها، منها ما يتعلق بالدليل الرقمي نفسه، ومنها ما يرتبط باقتناع القاضي.

**1- الشروط المرتبطة بالدليل الرقمي:** يشترط في الدليل الرقمي الذي يستند عليه القاضي الجنائي في بناء حكمه أن تتوافر فيه عدة ضوابط قانونية أهمها أن يكون مشروعا وقد تم طرحه في الجلسة للمناقشة.

– **مشروعية الدليل الرقمي:** يشترط في الدليل الالكتروني، الذي يعتمد عليه القاضي الجنائي في بناء حكمه في جريمة الإرهاب الرقمي، أن يكون مشروعا بحيث تتوافر فيه كل الشروط القانونية التي تسمح بقبوله في الدعوى، ونلاحظه أن المشرع لم يحدد بشكل صريح شروط قبول الدليل الرقمي، غير أن نص الفقرة الثانية من المـــــادة 6 من القـــــانون رقم 09-04[37] تعكس حرص المشرع على ضرورة السهر على حمـــاية وسلامة المعطيات" يجب في كل الأحوال على السلطة التي تقوم بالتفتيش والحجز السهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية ".

نفهم مما سبق أن الدليل بما فيه الرقمي متى كان غير مشروع، يؤدي حتما إلى فقدانه للمشروعية، ومنه عدم صلاحيته كدليل إثبات في الجريمة، وهو ما أكد عليه المشرع صراحة بموجب المادة 160 من قانون الإجراءات الجزائية " تسحب من ملف التحقيق أوراق الإجراءات التي أبطلت وتودع لدى قلم كتاب المجلس القضائي، ويحضر الرجوع إليها لاستنباط عناصر أو اتهامات ضد الخصوم في المرافعات وإلا تعرضوا لجزاء تأديبي بالنسبة للقضـــــاة ومحاكمة تأديبية للمحاميين المدافعين أمام مجلسهم التأديبي "، فهذا النص يعكس إرادة المشرع الصريحة في استبعاد الأدلة غير المشروعة، ومنه حتى الأدلة الرقمية غير المشروعة، تستبعد أيضا وفقا للقواعد العامة.

– **مناقشة الدليل الرقمي:** لا يجوز للقاضي أن يؤسس حكمه على دليل لم يطرح للمناقشة في جلسة المحاكمة، ولم يمنح للخصوم فرصة الاطلاع عليه ومناقشته، لأن مناقشة الدليل في الجلسة يعد من أهم الضوابط الإجرائية الواجب احترامها في الدليل الجنائي، وهذا ما نص عليه المشرع بموجب المادة 2/212 من قانون الإجراءات الجزائية كما يلي " ولا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضوريا أمامه ".

---

[37] - قانون رقم 09-04، مؤرخ في 5 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، مرجع سابق.

يطبق هذا الضابط على جميع الأدلة الرقمية المتحصل عليها من بيئة تكنولوجيا المعلومات، وهذا تطبيقا لمبدأين أساسيين هما شفوية المحاكمة واحترام حقوق الدفاع، اللذان يعتبران من المبادئ الأساسية التي يترتب على إغفالها بطلان إجراءات المحاكمة، وفقا لقاعدة ما بني على باطل فهو باطل؛ وإضافة إلى ضرورة مشروعية الدليل ومناقشته، يجب أيضا أن يكون الدليل الجنائي له أصل في أوراق الدعوى، فقاضي الموضوع له سلطة في تقدير أدلة الإثبات دون معقب متى ثبت أن الدليل الذي استند إليه له أصل ثابت في أوراق الدعوى.

**2- شروط لها علاقة باقتناع القاضي:** يعد القاضي الجنائي حرا في الاقتناع بالدليل الرقمي، وفقا لما يمليه عليه وجدانه، غير أنه من جهة أخرى، يجد نفسه مقيدا بشروط معينة أهمها:

- **تأسيس الاقتناع بالدليل الرقمي على الجزم واليقين:** تبنى الأحكام الجزائية على الجزم واليقين، لا على الظن والشك؛ ويستمد اليقين القضائي أساسه من قرينة البراءة التي تقضي بأن المتهم بريء إلى أن تثبت إدانته بموجب حكم قضائي بات[38]، ومنه يجب على القاضي أن يؤسس حكمه على الجزم واليقين، ولا يكتفي بمجرد الشك والاحتمال، لأن ذلك يفرض عليه تطبيق قاعدة الشك يفسر لصالح المتهم[39].

تجب الإشارة إلى أن اليقين القضائي المطلوب توافره في مجال الإثبات في المسائل الجزائية، هو اليقين النسبي القائم على التسبيب، وليس اليقين المطلق الذي هو بعيد عن سمات البشر[40]، وهذا ما يدفعنا للقول أن الأدلة الرقمية متى كانت مشروعة وثبت وجودها في أوراق الدعوى وتم مناقشتها في الجلسة، تعتبر أدلة علمية قطعية، ما يجعل اقتناع القاضي الجنائي بها يبلغ درجة اليقين، غير أن بلوغ القاضي درجة اليقين بالدليل الرقمي يستلزم ضرورة مناقشته له وفي هذا يكون دور القاضي محدودا بسبب عدم درايته بالأمور الفنية والتقنية لهذا يجب أن يكون للقاضي الجنائي خبرة في التعامل مع تقنية المعلومات[41] وأن يتمتع بكفاءة عالية في المجال التقني، وبهذا يتسنى له مناقشة الدليل الجنائي بكل عناصره، وهذه الدراية يمكن أن يطالها القاضي الجنائي من خلال عقد دورات تكوينية في هذا المجال.

- **الاقتناع بالدليل الرقمي وفقا لمقتضيات العقل والمنطق السليم:** فمهما كان القاضي حرا في اقتناعه بالدليل إلا أنه ينبغي عليه أن يؤسس حكمه على دليل يتماشى مع مقتضيات العقل والمنطق، فلابد أن يكون الدليل الرقمي الذي اقتنع به القاضي يؤدي بشكل منطقي ومعقول، إلى الحكم الذي نطق به في القضية.

---

[38] - " - كل شخص يعتبر بريئا ما لم تثبت إدانته بحكم قضـــــــائي حائز لقوة الشيء المقضي فيه "، المادة 1/1 من قانون رقم 17-07، مؤرخ في 27 مارس 2017، يعدل ويتمم أمر رقم 66- 155، مؤرخ في 8 يونيو 1966، يتضمن قانون الإجراءات الجزائية، ج. ر عدد 20، مؤرخة في 29 مارس 2017.

[39] - " - أن يفسر الشك في كل الأحوال لصـــــالح المتهم "، المـــــادة 5/1 من قـــــانون رقم 17-07، مؤرخ في 27 مارس 2017، يعدل ويتمم أمر رقم 66- 155، مؤرخ في 8 يونيو 1966، يتضمن قانون الإجراءات الجزائية، المرجع نفسه.

[40] - مروك نصر الدين، محاضرات في الإثبات الجنائي، الجزء الأول، د. ط، دار هومه، الجزائر، 2003، ص. 493.

[41] - عبد الرحيم زضاكي، " الدليل الالكتروني في المجال الجنائي "، مجلة البوغاز للدراسات القانونية والقضائية، الرباط، العدد 11، يناير 2021، ص. ص. 24، 25.

**الخاتمة:**

تعد جريمة الإرهاب الالكتروني من الجرائم المعاصرة والعابرة للحدود، والتي تعتمد في ارتكابها على التطور التكنولوجي وشبكة الانترنيت؛ ويشكل هذا النمط من الإجرام تهديدا خطيرا للسلم والأمن الدوليين؛ ومن أهم خصائص هذه الجريمة تميزها بالسرية وصعوبة الكشف عنها، والوصول إلى دليل يدين الإرهابيين المتورطين في ارتكابها؛ من هنا كان لزاما على الدول إعادة النظر في سياستها الداخلية لمكافحة هذه الجريمة وتعزيز سياسة الكشف عنها، لاسيما أمام عجز السياسة التقليدية في تحقيق الهدف المنشود؛ وهذا ما قام به المشرع الجزائري بموجب القانونين رقم 06-22 المعدل والمتمم لقانون الإجراءات الجزائية والقانون رقم 09-04؟؟؟؟؟؟؟؟، حيث واكب المشرع التطور التكنولوجي الحاصل في مجال ارتكاب الجريمة الإرهابية واعتمد بموجب هذين القانونين الوسائل التقنية لمكافحة جريمة الإرهاب المعلوماتي.

من بين الوسائل التقنية الحديثة التي اعتمدها المشرع لمكافحة هذا النوع الخطير من الإجرام، نجد المراقبة الإلكترونية أو ما يعرف باعتراض المراسلات وتسجيل الأصوات والتقاط الصور، وأيضا التفتيش المعلوماتي أو ما عبر عنه المشرع بموجب القانون رقم 09-04 بتفتيش المنظومات المعلوماتية.

تصطدم هذه التقنيات الحديثة بأهم حق من حقوق الإنسان المعترف بها دوليا، وهو الحق في حرمة الحياة الخاصة، لذا أكد المشرع على ضرورة تقييد عملية اللجوء إلى هذه الترتيبات بضوابط قانونية أهمها الحصول على إذن من الجهة القضائية المختصة؛ غير أن ما تم التوصل إليه من خلال هذه الدراسة أن القانون رقم 09-04 يجيز اللجوء لهذه الترتيبات حتى قبل وقوع الجريمة، وذلك من باب الوقاية من وقوعها، وهو ما يعد من قبيل المساس بحقوق الأفراد وحرمة حياتهم الخاصة، وإذا كانت خطورة الجرائم الإرهابية وتداعياتها الخطيرة على مختلف المجالات، هي ما يبرر للمشرع السماح باللجوء لهذه الترتيبات التقنية قبل وقوع الجريمة من باب الوقاية خير من العلاج، غير أن الموازنة بين الحق في حرمة الحياة الخاصة للأفراد وضرورة الكشف عن الجريمة الإرهابية، يقتضي على الأقل ضرورة وجود احتمالات قوية على وقوع الجريمة، للسماح باللجوء لمثل هذه الإجراءات التقنية الخطيرة على حقوق الإنسان.

تم التطرق من خلال هذه الدراسة لمسألة في غاية الأهمية، ما ساهم في طرحها ووجودها هو التطور التكنولوجي، إذ أن السماح باللجوء لإعمال الوسائل التكنولوجية للكشف عن الجرائم، أفرز إلى الساحة القانونية ما يعرف بالدليل الرقمي، وبالتالي طرح مسألة القيمة القانونية لهذا الدليل أمام القاضي الجنائي؛ وأمام سكوت المشرع عن هذه المسألة يتم العودة لإعمال القواعد العامة المعمول بها في قانون الإجراءات الجزائية، التي تقضي بخضوع الأدلة الرقمية للسلطة التقديرية للقاضي الجنائي، هذه السلطة التي تعد مقيدة بضرورة مشروعية الحصول على الدليل وضرورة مناقشته في الجلسة احتراما لمبدأي الشفوية والحق في الدفاع، غير أن مناقشة الدليل الرقمي يقتضي الاهتمام بمسألة في غاية الأهمية وهي تكوين القضاة من حيث الجانب التقني والعلمي لبلوغ درجة الاقتناع اليقيني بالدليل الرقمي.