دور الضبط الإداري الإلكتروني في مكافحة التنمر الإلكتروني: دراسة تحليلية مقارنة

The Role of Electronic Administrative Control in Combating Cyberbullying: A Comparative Analytical Study

دكتور

عادل السيد محمد علي

مدرس القانون

المعهد العالي للعلوم الإدارية بجناكليس- البحيرة

ملخص البحث

شهد العالم في العقود الأخيرة تحولًا جذريًا بفعل الثورة التكنولوجية، التي أدت إلى ظهور جرائم جديدة عابرة للحدود تعرف بـ "الجرائم المعلوماتية"، ومن بين هذه الجرائم، تبرز جريمة التنمر الإلكتروني كواحدة من أخطر التحديات التي تهدد الأمن الاجتماعي والنظام العام في المجتمع الرقمي؛ نظرًا لقدرتها على الانتشار السريع والوصول إلى عدد كبير من الضحايا دون قيود جغرافية.

وأمام هذه التحديات المتزايدة، يقع على عاتق هيئات الضبط الإداري مسؤولية جوهرية لمواجهة التنمر الإلكتروني، ويتطلب ذلك تبني تدابير قانونية وتنظيمية صارمة لضبط حقوق وحريات الأفراد عند ممارستهم لأنشطتهم عبر الإنترنت؛ لذلك وضعت الدول قوانين جديدة أو عدلت القوانين القائمة لمواجهة هذه التحديات المستجدة، مع التأكيد على ضرورة التعاون بين مختلف الهيئات المعنية لضمان فعالية هذه الجهود.

ومع ذلك، تواجه هيئات الضبط الإداري تحديات كبيرة في مكافحة التنمر الإلكتروني، من بينها صعوبة مواكبة التطورات التكنولوجية السريعة، وصعوبة تتبع الجرائم عبر الشبكات المعقدة؛ لذلك تحتاج هذه الهيئات إلى تكثيف جهودها وتبني تقنيات حديثة وتطوير التشريعات وتعزيز التعاون الدولي؛ لضمان بيئة رقمية آمنة تحمي حقوق الأفراد وتصون كرامتهم.

وتتجلى أهمية البحث في استقصاء الطبيعة القانونية لجريمة التنمر الإلكتروني، وتحديد خصائصها وأنواعها، ووضع السبل القانونية والتدابير التي يمكن لسلطات الضبط الإداري الإلكتروني تبنيها لمواجهة هذه الجريمة. وقد تم استخدام المنهج الوصفي التحليلي والمقارن عند إعداد هذا البحث.

لذلك جاء البحث بعنوان: "دور الضبط الإداري الإلكتروني في مكافحة التنمر الإلكتروني: دراسة تحليلية مقارنة"، وتناولته من خلال مقدمة، ومبحثين، وخاتمة.

أما المبحث الأول، تناولت فيه: مفهوم الضبط الإداري الإلكتروني وهيئاته، ومفهوم التنمر الإلكتروني وأسبابه وآثاره السلبية.

والمبحث الثاني، فقد ذكرت فيه: الإطار التشريعي لمواجهة التنمر الإلكتروني، ووسائل الضبط الإداري الإلكتروني في مواجهة التنمر الإلكتروني، وإجراءات الضبط الإداري الإلكتروني لمواجهة التنمر الإلكتروني. ثم اختتمت بحثي بما توصلت إليه من نتائج وتوصيات.

الكلمات المفتاحية:

الضبط الإداري الإلكتروني– التنمر الإلكتروني– التحرش المعنوي– وسائل الضبط الإداري الإلكتروني– إجراءات الضبط الإداري الإلكتروني.

Abstract

In recent decades, the world has witnessed a radical transformation due to the technological revolution, which has led to the emergence of new cross-border crimes known as "cybercrimes." Among these crimes, cyberbullying stands out as one of the most serious challenges threatening social security and public order in the digital society, given its ability to spread rapidly and reach a large number of victims without geographical constraints.

In the face of these increasing challenges, administrative control bodies bear a fundamental responsibility to combat cyberbullying. This requires the adoption of strict legal and regulatory measures to regulate the rights and freedoms of individuals when engaging in online activities. Therefore, countries have enacted new laws or amended existing ones to address these emerging challenges, with an emphasis on the necessity of cooperation among various concerned bodies to ensure the effectiveness of these efforts.

However, administrative control bodies face significant challenges in combating cyberbullying, including the difficulty of keeping pace with rapid technological advancements and the challenge of tracking crimes across complex networks. As a result, these bodies need to intensify their efforts, adopt modern technologies, develop legislation, and enhance international cooperation to ensure a secure digital environment that protects individuals' rights and preserves their dignity.

The importance of this research lies in exploring the legal nature of the crime of cyberbullying, identifying its characteristics and types, and establishing the legal methods and measures that electronic administrative control authorities can adopt to combat this crime. The descriptive, analytical, and comparative method was used in preparing this research.

Therefore, the research is titled: "The Role of Electronic Administrative Control in Combating Cyberbullying: An Analytical Comparative Study," and it is discussed through an introduction, two chapters, and a conclusion.

The first chapter addresses the concept of electronic administrative control and its authorities, the concept of cyberbullying, its causes, and its negative effects.

The second chapter discusses the legislative framework for combating cyberbullying, the means of electronic administrative control in combating cyberbullying, and the procedures for electronic administrative control in combating cyberbullying. The research concludes with the findings and recommendations.

Keywords:

Electronic Administrative Control – Cyberbullying – Psychological Harassment – Means of Electronic Administrative Control – Procedures of Electronic Administrative Control.

مقدمة

شهد العالم في العقود الأخيرة ثورة تكنولوجية هائلة أدت إلى تغيير جذري في كافة جوانب الحياة اليومية، من الاتصالات والمعاملات إلى المعرفة والاقتصاد، ومع هذا التقدم التكنولوجي ظهرت جرائم جديدة عابرة للحدود تعرف بالجرائم المعلوماتية، التي تشمل مجموعة واسعة من الأفعال الضارة التي ترتكب عبر الفضاء الرقمي، وتبرز من بين هذه الجرائم، جريمة التنمر الإلكتروني كأحد التحديات الكبرى التي تهدد الأمن الاجتماعي والنظام العام في المجتمع المعلوماتي.

فتُعد جريمة التنمر الإلكتروني من الجرائم العمدية التي تهدف إلى إلحاق الأذى النفسي أو الاجتماعي بالآخرين من خلال استخدام الوسائل الإلكترونية، وتتمثل خطورة هذه الجريمة في قدرتها على الانتشار السريع والوصول إلى عدد كبير من الضحايا دون قيود جغرافية، مما يجعلها تهديدًا مباشرًا للنظام العام وللسلم الاجتماعي في الفضاء الرقمي. ولا يقتصر تأثير هذه الجريمة على الأفراد المتضررين فحسب، بل يمتد ليشمل المجتمع ككل من خلال تعزيز بيئة رقمية غير آمنة وغير موثوقة.

وأمام هذه التحديات المتنامية، تتحمل هيئات الضبط الإداري مسؤولية حيوية تتمثل في حماية الفضاء المعلوماتي من الجرائم الإلكترونية، بما في ذلك جريمة التنمر الإلكتروني، وتقتضي هذه المسؤولية اتخاذ تدابير قانونية وتنظيمية صارمة تهدف إلى ضبط حقوق وحريات الأفراد عند ممارستهم لأنشطتهم عبر الإنترنت، مع مراعاة أن هذه الحقوق مكفولة دستوريًا، وخاصةً أن الأساليب التقليدية للضبط الإداري، التي تعتمد على أدوات ووسائل ذات طبيعة مادية، غالبًا ما تثبت عدم فاعليتها في التعامل مع الجرائم الإلكترونية، التي تتميز بوقوعها في بيئة افتراضية تتسم بقدر كبير من المرونة والتعقيد، مما يتطلب استراتيجيات ضبط أكثر تطورًا تتناسب مع طبيعة هذه الجرائم.

واستجابة لهذا التحديات، قامت العديد من الدول بسن قوانين جديدة تهدف إلى مكافحة جريمة التنمر الإلكتروني، أو على الأقل بتعديل القوانين القائمة لتتوافق مع طبيعة الجرائم الإلكترونية المستجدة، وتهدف هذه القوانين إلى توفير إطار قانوني يحدد الجرائم والعقوبات المترتبة عليها، ويضع آليات فعالة لرصد ومنع هذه الجرائم من خلال التعاون بين مختلف الهيئات والمؤسسات المعنية.

ومما يجدر التنويه به، أن هيئات الضبط الإداري تتحمل مسؤولية تحقيق التوازن الدقيق بين واجبها في الحفاظ على النظام العام بعناصره الثلاثة: الأمن العام، والصحة العامة، والسكينة العامة، وبين حماية حقوق وحريات الأفراد. وتخضع هذه الهيئات في أداء مهامها لرقابة القضاء الإداري، الذي يضمن عدم تجاوزها للصلاحيات المخولة لها قانونًا، ويعمل على حماية الحقوق الدستورية للأفراد من أي تعسف أو تجاوز.

غير أن القيام بمهام الضبط الإداري في مجال مكافحة التنمر الإلكتروني ليس بالأمر اليسير؛ إذ تواجه هذه الهيئات العديد من التحديات والصعوبات التي تعيق أداءها بفعالية، ومن أبرز هذه التحديات، عدم قدرة الهيئات على مواكبة التطورات السريعة في مجال التكنولوجيا، وصعوبة تتبع الجرائم المرتكبة عبر شبكات معقدة ومتشابكة، وإضافة إلى ذلك، يشكل التعاون الدولي متطلبًا أساسيًا لمكافحة هذه الجرائم، إلا أن اختلاف الأنظمة القانونية بين الدول يمثل تحديًا إضافيًا.

وتأسيسًا على ذلك، يتعين على هيئات الضبط الإداري الإلكتروني بذل جهود مضاعفة لتعزيز قدراتها في مواجهة جريمة التنمر الإلكتروني، وذلك من خلال تبني تقنيات حديثة، وتطوير التشريعات، وتعزيز التعاون الدولي، فكلما تعززت هذه الجهود، كلما انخفضت الآثار السلبية لهذه الجريمة، مما يسهم في خلق بيئة رقمية آمنة تحمي حقوق الأفراد وتصون كرامتهم.

أولًا: أهمية البحث وأسباب اختياره

في الآونة الأخيرة، شهدت ظاهرة التنمر الإلكتروني انتشارًا واسعًا على منصات التواصل الاجتماعي، وبرامج التراسل الفوري الإلكترونية، والمدونات، وغرف الدردشة الإلكترونية، حيث أصبحت تشكل أحد أبرز أشكال العنف الإلكتروني والإيذاء السيبراني، خاصةً بين فئات الأطفال والمراهقين، ويتسم هذا النوع من التنمر باستمراريته وقدرته على إلحاق أضرار نفسية جسيمة، تتراوح بين القلق والاكتئاب، وقد تصل في بعض الحالات إلى دفع الضحايا نحو الانتحار.

وفي ضوء التزايد المطرد في حجم وانتشار ظاهرة التنمر الإلكتروني بين أفراد المجتمع، وتنوع أشكالها وأساليبها، وما يصاحبها من تداعيات خطيرة تهدد أمن واستقرار المجتمعات، تبرز الحاجة الملحة لتناول هذه الظاهرة بالبحث والتحليل. ويتطلب ذلك استقصاء الطبيعة القانونية للتنمر الإلكتروني، واستعراض خصائصه وأنواعه، وتحديد السبل القانونية والتدابير التي يمكن لسلطات الضبط الإداري الإلكتروني أن تعتمدها لمواجهة هذه الظاهرة الإجرامية الخطيرة التي تهدد النظام العام وسلامة الأفراد في المجتمع الرقمي.

ثانيًا: إشكالية البحث

تتمثل إشكالية البحث في السعي نحو تطوير آلية قانونية فعّالة وملائمة لتعزيز دور هيئات الضبط الإداري في الدولة، بهدف حماية النظام العام من مخاطر جريمة التنمر الإلكتروني، ويتطلب ذلك إيجاد توازن دقيق بين حق الإدارة في حماية النظام العام من جهة، وحق الأفراد في ممارسة حقوقهم وحرياتهم من جهة أخرى. ولتحقيق هذا التوازن، يستلزم الأمر وضع تدابير احترازية وضمانات وقائية فعالة تحد من ارتكاب هذه الجريمة، دون المساس بالحقوق والحريات المكفولة دستوريًا.

ومن ثم، تتمحور إشكالية البحث حول الإجابة على التساؤلات الآتية:

- ما هو مفهوم الضبط الإداري الإلكتروني وما هي الهيئات المسؤولة عن تطبيقه؟
- ما هو مفهوم التنمر الإلكتروني وما هي أبرز أسبابه وآثاره السلبية على الأفراد والمجتمعات؟
- ما هو الإطار التشريعي الذي يحكم مواجهة التنمر الإلكتروني؟
- مدى كفاية القوانين والأنظمة في مكافحة التنمر الإلكتروني؟
- ما هي الوسائل والأدوات المتاحة للضبط الإداري الإلكتروني في مواجهة التنمر الإلكتروني؟
- ما هي الإجراءات العملية التي تتخذها هيئات الضبط الإداري الإلكتروني في التصدي للتنمر الإلكتروني، ومدى فعاليتها في الحد من هذه الظاهرة؟
- ما هي أبرز التحديات التي تواجه هيئات الضبط الإداري الإلكتروني في التصدي لظاهرة التنمر الإلكتروني، وكيفية التغلب عليها؟

ثالثًا: أهداف البحث

يهدف هذا البحث إلى تحقيق مجموعة من الأهداف الجوهرية، وفي مقدمتها تطبيق المبادئ الأساسية لنظرية الضبط الإداري التقليدية على متطلبات الفضاء الإلكتروني، بما في ذلك مواجهة جريمة التنمر الإلكتروني، باعتباره مجالًا حديثًا يستدعي تكييف سلطات الضبط الإداري الإلكتروني، وتأتي هذه الجهود استجابة للتحولات الجذرية التي أحدثتها الثورة الرقمية، والتي أثرت بشكل عميق على البنية التنظيمية والوظيفية لهيئات الضبط الإداري، فلم يعد الطابع السيادي التقليدي للضبط الإداري كافيًا لمواجهة التحديات المستجدة، خاصة مع ظهور فاعلين جدد، مثل

الشركات الخاصة التي تتحكم في منصات التواصل الاجتماعي وتضع معايير استخدام الفضاءات الإلكترونية، والتي قد تتجاوز في بعض الأحيان الصلاحيات الضبطية الرسمية.

كما يهدف هذا البحث إلى تقديم رؤية متكاملة وشاملة حول فعالية وسائل الضبط الإداري الإلكتروني في الحد من ظاهرة التنمر الإلكتروني وضمان حماية الأفراد في الفضاء الرقمي، ويسعى أيضًا إلى الاستفادة من التجارب المقارنة بين النظامين المصري والفرنسي، من خلال تحليل نقاط القوة والضعف في كل منهما، واستخلاص الدروس المستفادة. وبناءً على ذلك، يقدم البحث توصيات عملية تهدف إلى تعزيز الإطار القانوني والإداري المتعلق بمكافحة التنمر الإلكتروني، بما يضمن تطوير سياسات أكثر فعالية لتحقيق التوازن بين حماية حقوق الأفراد وضمان الأمن الرقمي.

رابعًا: منهج البحث

اعتمد الباحث على المنهج الوصفي التحليلي لدراسة وتحليل النصوص القانونية والأطر التنظيمية للضبط الإداري الإلكتروني في مكافحة التنمر الإلكتروني في النظامين المصري والفرنسي، حيث تم وصف الوقائع القانونية وتحليلها بدقة للوصول إلى فهم شامل لطبيعة وآليات الضبط الإداري الإلكتروني ومدى فعاليتها. كما تم استخدام المنهج المقارن لمقارنة الإجراءات والوسائل المتبعة في النظامين المصري والفرنسي، وتحليل أوجه التشابه والاختلاف بينهما؛ بهدف استخلاص أفضل الممارسات وتقييم فعالية كل نظام في مكافحة التنمر الإلكتروني.

خامسًا: الدراسات السابقة

1- **الدراسة الأولى** بعنوان: "دور الضبط الإداري في الحد من مخاطر الفضاء الإلكتروني في مصر وفرنسا"، للأستاذ الدكتور/ حسين مقداد عبد اللطيف، بحث منشور بمجلة العلوم القانونية والاقتصادية، العدد الأول، السنة الخامسة والستون، كلية الحقوق، جامعة عين شمس، يناير 2023م.

وقد هدفت هذه الدراسة إلى توضيح دور الضبط الإداري في حماية أمن الفضاء الإلكتروني باعتباره الامتداد الطبيعي للأمن القومي للدولة في النظامين المصري والفرنسي. وقد توصلت الدراسة إلى عدة نتائج، من أبرزها: أن فكرة الفضاء العلني لم تدخل بعد ضمن أدبيات القانون الإداري، وخاصةً في مجال الضبط الإداري، رغم أن هذا الفضاء يشكل المجال الطبيعي لسلطة الضبط الإداري في تنظيم العلاقة بين الأفراد عبر وسائل الاتصال، كما توسعت ولاية الضبط الإداري لتشمل كافة المخاطر والتهديدات التي تمس النظام العام، بغض النظر عن طبيعتها.

ومن أهم التوصيات التي خلصت إليها الدراسة: إصدار قانون لحماية أمن الفضاء السيبراني، ليكون الإطار المرجعي لسلطة الإدارة الضبطية في تنظيم النشاط الإنساني عبر الفضاء الإلكتروني.

وتتشابه هذه الدراسة مع دراستنا في تناول دور هيئات الضبط الإداري الإلكتروني في الحد من مخاطر الفضاء الإلكتروني في النظامين المصري والفرنسي، إلا أنها تختلف في تناولها للفضاء الإلكتروني بشكل عام، بينما ركزت دراستنا على بيان دور هيئات الضبط الإداري الإلكتروني في مكافحة التنمر الإلكتروني بشكل خاص، وذلك في النظامين المصري والفرنسي.

2- **الدراسة الثانية** بعنوان: "دور الضبط الإداري الإلكتروني في مكافحة الجرائم المعلوماتية: دراسة مقارنة"، للباحث/ عماد جاسم حسين الشنكالي، وهي رسالة ماجستير، مقدمة إلى كلية الحقوق، جامعة تكريت، العراق، 2022م.

وقد هدفت هذه الدراسة إلى توضيح دور أجهزة الضبط الإداري الإلكتروني في مكافحة الجرائم المعلوماتية في النظامين العراقي والمصري والجزائري. وقد خلصت الدراسة إلى العديد من النتائج، منها أن مكافحة الجرائم المعلوماتية تتطلب تضافر الجهود الدولية بالإضافة إلى ما تقوم به الدول من إجراءات وفقًا لتشريعاتها الوطنية، خاصة في ظل تزايد الهجمات السيبرانية. ومن أبرز التوصيات التي توصلت إليها هذه الدراسة: تعزيز التعاون الدولي في مجال مكافحة الجرائم المعلوماتية، والاستفادة من تجارب الدول الرائدة في هذا المجال، بما يعزز من فعالية الجهود المبذولة في مكافحة هذه الجرائم.

وتتشابه هذه الدراسة مع دراستنا في تناول دور هيئات الضبط الإداري الإلكتروني في مكافحة الجرائم المعلوماتية في النظام المصري، لكنها تختلف في تناولها لمكافحة الجرائم المعلوماتية بشكل عام في النظامين العراقي والجزائري، بينما تركز دراستنا على دور هيئات الضبط الإداري الإلكتروني في مكافحة التنمر الإلكتروني بشكل خاص، وذلك في النظامين المصري والفرنسي.

سادسًا: خطة البحث

ينقسم هذا البحث إلى: مقدمة، ومبحثين، وخاتمة، والمراجع، وذلك على النحو الآتي:

- **أما المقدمة فقد اشتملت على:** أهمية البحث، وإشكالية البحث، وأهداف البحث، ومنهج البحث، والدراسات السابقة، وخطة البحث.

- **المبحث الأول: مفهوم الضبط الإداري الإلكتروني والتنمر الإلكتروني.**

<u>وفيه مطلبان:</u>

  - **المطلب الأول:** مفهوم الضبط الإداري الإلكتروني وهيئاته.
  - **المطلب الثاني:** مفهوم التنمر الإلكتروني وأسبابه وآثاره السلبية.
- **المبحث الثاني: سلطات الضبط الإداري الإلكتروني في مواجهة التنمر الإلكتروني.**

<u>وفيه ثلاثة مطالب:</u>

  - **المطلب الأول:** الإطار التشريعي لمواجهة التنمر الإلكتروني.
  - **المطلب الثاني:** وسائل الضبط الإداري الإلكتروني في مواجهة التنمر الإلكتروني.
  - **المطلب الثالث:** إجراءات الضبط الإداري الإلكتروني لمواجهة التنمر الإلكتروني.
- **الخاتمة:** وتشمل: النتائج والتوصيات.
- **المراجع.**

المبحث الأول

مفهوم الضبط الإداري الإلكتروني والتنمر الإلكتروني

تمهيد وتقسيم:

يشهد العالم تحولًا نوعيًا في استخدامات التكنولوجيا، مما يستدعي إعادة النظر في الأطر القانونية والتنظيمية لضمان حماية النظام العام في الفضاء الرقمي. ويُعد الضبط الإداري الإلكتروني أحد الأدوات الأساسية التي تتبناها الدول لمواجهة التحديات المستجدة، ومنها التنمر الإلكتروني الذي يُمثل تهديدًا حقيقيًا للنظام العام.

حيث يُحدث التنمر الإلكتروني خللًا في العلاقات الاجتماعية ويزيد من معدلات العنف النفسي والاجتماعي، ويؤدي التنمر الإلكتروني إلى تقويض الثقة في الفضاء الرقمي، ما ينعكس سلبًا على الأمن والسلم الاجتماعيين. بالإضافة إلى ذلك، يمكن أن يتسبب التنمر الإلكتروني في تعطل الأنشطة التعليمية والمهنية، ويخلق بيئة من الخوف وعدم الأمان بين المستخدمين.

وفي ظل هذه التحديات، يصبح الضبط الإداري الإلكتروني أداة حيوية لضمان تطبيق القانون وحماية الأفراد من الاعتداءات الرقمية، وذلك من خلال رصد الأنشطة المشبوهة، وتقديم المساعدة للضحايا، ومعاقبة المتورطين في هذه الجرائم.

ويهدف هذا المبحث إلى تقديم تحليل دقيق لمفاهيم الضبط الإداري الإلكتروني والتنمر الإلكتروني، مع التركيز على كيفية تأثير التنمر الإلكتروني على النظام العام، وذلك في مطلبين على النحو الآتي:

- **المطلب الأول: مفهوم الضبط الإداري الإلكتروني.**
- **المطلب الثاني: مفهوم التنمر الإلكتروني.**

المطلب الأول

مفهوم الضبط الإداري الإلكتروني وهيئاته

وفيه فرعان:

- **الفرع الأول:** مفهوم الضبط الإداري الإلكتروني.
- **الفرع الثاني:** هيئات الضبط الإداري الإلكتروني.

الفرع الأول

مفهوم الضبط الإداري الإلكتروني

أولًا- تعريف الضبط الإداري الإلكتروني:

بادئ ذي بدء، يتطلب هذا الموضوع بيان مفهوم الضبط الإداري أولًا، من الناحية التشريعية والفقهية، ثم بيان مفهوم الضبط الإداري الإلكتروني؛ وذلك لإبراز علاقة الترابط بين نظرية الضبط الإداري والضبط الإداري الإلكتروني، وذلك على النحو الآتي:

1- التعريف التشريعي للضبط الإداري:

من الملاحظ أن المشرع في كل من فرنسا ومصر لم يتعرض لتعريف محدد للضبط الإداري بصورة قاطعة، وإنما اكتفى بسرد أغراضه. وفي نطاق تناوله لأغراضه، لم يتعرض لتحديد هذه الأغراض بصورة واضحة ومحددة. وسوف نستعرض تعريف المشرع الفرنسي والمشرع المصري للضبط الإداري على النحو الآتي:

أ. تعريف المشرع الفرنسي للضبط الإداري:

منذ قيام الثورة الفرنسية وصدور التشريعات، لم تُحدد أغراض الضبط الإداري بصورة قاطعة وإنما بصورة استدلالية؛ فقد نص المرسوم الصادر في 14 ديسمبر سنة 1789 في المادة (50) على اختصاص الهيئات المحلية، إذ يقع على عاتقها: "أن تجعل السكان ينعمون بمزايا ضبط حسن، وخاصة النظافة والصحة والأمن بالشوارع والأماكن والمنشآت العامة". كما نصت المادة (97) من القانون الصادر عام 1884، والخاص بتحديد اختصاصات الهيئات المحلية، على

أنه: "يختص البوليس المحلي بالمحافظة على حسن النظام والأمن العام والصحة العامة"[1].

ومن الملاحظ على النص السابق عرضه أنه لم يرد فيه ذكر للسكينة العامة، التي هي أحد الالتزامات الأساسية للضبط الإداري. وبذلك، تكون الأغراض المذكورة في المواد السابقة على سبيل الاستدلال وليس الحصر؛ لذلك، نجد أن المشرع الفرنسي اتجه إلى النص في القانون الحالي الخاص بالضبط المحلي الصادر في 2 مارس 1982 في المادة (212) على ذكر السكينة العامة كأحد أغراض الضبط الإداري. ومع ذلك، يبقى التعريف غير محدد بصورة قاطعة[2].

ب. تعريف المشرع المصري للضبط الإداري:

أما فيما يتعلق بموقف المشرع المصري، نجد أنه صدرت قوانين عديدة نصت على الضبط الإداري، لكنها نصت على مضمونه بشكل عام، أو تناولت أجهزة الضبط الإداري، دون إيراد تعريف محدد لذلك، ومنها التشريعات التي صدرت لتنظيم هيئة الشرطة، حيث لم تحدد الضبط بصورة واضحة ومحددة. فالمادة (3) من القانون رقم 234 لسنة 1955، وكذلك المادة (3) من القانون رقم 61 لسنة 1964، والمادة (3) من القانون رقم 109 لسنة 1971- القانون الحالي لهيئة الشرطة- تنص على أنه: "تختص هيئة الشرطة بالمحافظة على النظام العام والأمن والآداب وحماية الأرواح والأعراض والأموال، وعلى الأخص منع الجرائم وضبطها، كما تختص بكفالة الطمأنينة والأمن للمواطنين في المجالات كافة وتنفيذ ما تفرضه عليها القوانين واللوائح من واجبات".

وإذا كان المشرع المصري قد تناول العديد من أغراض الضبط الإداري، إلا أنه تناولها بصورة منتقدة نظرًا لتكراره لبعض أغراض الضبط. وكذلك نصت المادة (206) من الدستور المصري الحالي الصادر سنة 2014 على أنه: "الشرطة هيئة مدنية نظامية، في خدمة الشعب، وولاؤها له، وتكفل للمواطنين الطمأنينة والأمن، وتسهر على حفظ النظام العام، والآداب العامة، وتلتزم بما يفرضه عليها الدستور والقانون من واجبات، واحترام حقوق الإنسان وحرياته الأساسية، وتكفل الدولة أداء أعضاء هيئة الشرطة لواجباتهم، وينظم القانون الضمانات الكفيلة بذلك".

ويتضح من استقراء ما سبق، أن القانون المصري قد تناول كثيرًا الأغراض المتعلقة بالضبط

---

[1] أ. عماد جاسم حسين الشنكالي، دور الضبط الإداري الإلكتروني في مكافحة الجرائم المعلوماتية: دراسة مقارنة، رسالة ماجستير، كلية الحقوق، جامعة تكريت، العراق، 2022م، ص 8.

[2] (E) Picard, la nation de police administrative, thèse, Paris I, 1978, p.32.

الإداري، إلا أن هذه الأغراض جاءت في عبارات مبهمة، وبالتالي لم تحدد أغراض الضبط بصورة واضحة؛ ولعل ذلك يرجع بدوره إلى مرونة فكرة النظام العام والأمن العام والآداب العامة، مما جعل المشرع يعزف عن وضع تعريف محدد لفكرة الضبط الإداري خشية منه ألا يدرج إحدى الصور التي يجب أن تندرج تحت هذه المدلولات الثلاثة، فيقع الخلط والخلل[1].

ويمكن إرجاع مسلك المشرع المصري والفرنسي فيما يتعلق بعدم تحديد أغراض الضبط بصورة واضحة وقاطعة إلى مرونة ونسبية فكرة النظام العام؛ إذ تختلف هذه الفكرة باختلاف ظروف الزمان والمكان، فما قد يعد من الأفعال المضرة بالنظام العام في أحد الأوقات قد لا يكون كذلك بعد فترة من الزمن، وما يعد من النظام العام في بلد ما قد لا يعد كذلك في بلد آخر[2].

2- التعريف الفقهي للضبط الإداري:

ذهب بعض الفقه المصري إلى تعريف الضبط الإداري بأنه: النشاط الذي تتولاه الهيئات الإدارية، ويتمثل في تقييد النشاط الخاص بهدف صيانة النظام العام[3]. كما عرفه فقيه آخر بأنه: حق الإدارة في فرض قيود على الأفراد تحد من حرياتهم بقصد حفظ النظام العام[4]. وعُرف الضبط الإداري أيضًا بأنه: مجموعة من القواعد تفرضها سلطة عامة على الأفراد في حياتهم العادية أو لممارسة نشاط معين بقصد صيانة النظام العام، أي لتنظيم المجتمع تنظيمًا وقائيًا[5].

وعُرّف الضبط الإداري لدى بعض الفقه الفرنسي بأنه: نشاط إداري يهدف إلى الحفاظ على النظام العام، دون السعي على مرتكبي جريمة محددة أو القبض عليهم[6]. وهناك من يرى الضبط الإداري بأنه: الهيئات والأجهزة الإدارية التي تمارس هذه الوظيفة في إطار السلطة

---

[1] لمزيد من التفصيل يراجع: أ. عماد جاسم حسين الشنكالي، دور الضبط الإداري الإلكتروني في مكافحة الجرائم المعلوماتية، مرجع سابق، ص 9-10.

[2] د. محمد شريف إسماعيل، الضبط الإداري في الظروف الاستثنائية، رسالة دكتوراة، كلية الحقوق، جامعة عين شمس، 1979م، ص 10.

[3] د. محمود عاطف البنا، حدود سلطة الضبط الإداري، كلية الحقوق، جامعة القاهرة، 1980م، ص 4.

[4] د. سليمان محمد الطماوي، الوجيز في القانون الإداري، دار الفكر العربي، القاهرة، 1994م، ص 598.

[5] د. توفيق شحاتة، مبادئ القانون الإداري، دار النشر للجامعات المصرية، القاهرة، 1954م، ص 328.

[6] "La police administrative, c'est une activité qui vise à assurer le maintien de l'ordre public, sans tendre à la recherche ou à l'arrestation des auteurs d'une infraction déterminée". M. Coulibaly: La police administrative, Université Toulouse 1 Capitole, Toulouse, France, 2016-2017, p. 8.

التنفيذية، ومجموع الموظفين المكلفين بمهمة الضبط[1]. كما يُعرّف أيضًا بأنه: أحد أنشطة الإدارة العامة، والذي يستهدف الحفاظ على النظام العام، إما بمنع التجاوزات أو بوضع حد لها، مع احترام الحريات[2].

وبناءً على التعاريف السابقة، يمكن تعريف الضبط الإداري بأنه: مجموعة من الإجراءات والتدابير التي تتخذها السلطات الإدارية، والتي تتمثل في فرض قيود تنظيمية على الحريات العامة والخاصة للأفراد، بهدف الحفاظ على النظام العام بمختلف عناصره. ويتم ذلك من خلال تحقيق التوازن بين مصلحة المجتمع في الحفاظ على النظام العام وبين احترام الحقوق والحريات الأساسية للأفراد.

ونلاحظ من خلال التعاريف سالفة الذكر أن الضبط الإداري هو مجموعة من التدابير والإجراءات التي تظهر في شكل وسائل تدخل مختلفة لمواجهة الجرائم المعلوماتية بشكل عام والتنمر الإلكتروني بشكل خاص؛ فنجد أن السلطات الإدارية تتخذ تدابير وإجراءات متنوعة لمواجهة هذه الجرائم، وتشمل هذه التدابير إصدار قرارات تنظيمية وفردية، واستخدام القوة الجبرية لفرض القيود اللازمة على استخدام التكنولوجيا والإنترنت. ويكمن الهدف من هذه التدابير في حماية النظام العام من التهديدات التي تشكلها الجرائم المعلوماتية والتنمر الإلكتروني، وذلك من خلال تحقيق التوازن بين حماية المجتمع واحترام حقوق الأفراد وحرياتهم الأساسية. وتُتخذ هذه التدابير ضمن إطار قانوني يضمن المشروعية، وتتميز بكونها انفرادية وتقديرية ووقائية، مما يتيح للسلطات الإدارية المرونة اللازمة للتعامل مع التطورات السريعة في مجال التكنولوجيا الرقمية.

3- تعريف الضبط الإداري الإلكتروني:

جاء الضبط الإداري الإلكتروني كفكرة مستحدثة ضمن دراسات القانون الإداري الحديثة،

---

(1) R.Zouaimia, M.-Ch. Rouault, droit administratif, les sources et l'activité l' organization administrative principes généraux administrative – le contrôle de l' administration, BERTI edition, Alger, 2009, p.197.

(2) "La police administrative est une activité de l'administration publique dont la finalité est le maintien de l'ordre public, soit en en prévenant les atteintes, soit en y mettant fin, dans le respect des libertés". Dalloz, Police administrative, Juillet 2021. https://www.dalloz.fr/documentation/Document.

لتطبيق مفهوم الضبط الإداري التقليدي باستخدام الوسائل التكنولوجية الحديثة[1].

وعند تعريف الضبط الإداري الإلكتروني، ذهب بعض الفقه[2] إلى القول بأنه لا يختلف في جوهره عن مفهوم الضبط الإداري التقليدي، مع التأكيد على طابعه المستجد، فهو يمثل تنظيم وتقييد النشاط الفردي داخل المواقع الإلكترونية لحماية النظام العام. ويلاحظ على هذا التعريف أنه يتسم بالاختزال من ناحية، وبالقصور من ناحية أخرى؛ إذ يقتصر على نشاط الأفراد دون أن يشمل حرياتهم الرقمية. وعلى الرغم من استقرار جمهور فقه القانون الإداري على أن الضبط الإداري يشمل حريات الأشخاص وأنشطتهم على حد سواء، إلا أن هذا التعريف يعتمد على غايته فقط دون التعرض لمضمونه– حيث التدابير الاستثنائية التي ترد على حريات الأشخاص وأنشطتهم بغرض الحفاظ على النظام العام[3].

وعُـرّف أيضًـا الضـبط الإداري الإلكترونـي بأنـه: القيـود التـي تقتضـيها المصـلحة العامـة وتفرضها السلطة العامة على نشاط الأفراد عبر الواقع الإلكتروني لغرض حماية النظام العام[4].

كما عرفه بعض الفقه بأنه: مجموعة من الضوابط والقيود القانونية والتقنية التي ترد على حريات الأفراد وأنشطتهم الرقمية، بغرض الحفاظ على النظام العام، سواء كان مصدر هذه القيود إرادة المشرع أم إرادة الإدارة المستقلة[5].

---

[1] صحيح أن الإنترنت أدى إلى ظهور مظاهر جديدة للإخلال بالنظام العام وساهم في ارتكاب جرائم لم تكن موجودة من قبل، لكن في المقابل هناك من يؤيد أن الإنترنت يمكن أن يكون أداة لضبط المجرمين؛ حيث يساهم في ضبطهم من خلال توزيع صورهم وجمع المعلومات عنهم وتتبع تحركاتهم واهتماماتهم. لمزيد من التفاصيل يراجع: د. ناجح أحمد عبد الوهاب، التطور الحديث للقانون الإداري في ظل نظام الحكومة الإلكترونية، دار النهضة العربية، القاهرة، 2012م، ص 114.

[2] أ. محمد سليمان شبير، الإطار القانوني لسلطة الضبط الإداري الإلكتروني في فلسطين: دراسة تحليلية، مجلة جامعة الأزهر، المجلد 17، العدد 2 (ب)، غزة، فلسطين، 2015م، ص 314، بحث منشور على الموقع الآتي:

- **https://www.researchgate.net/profile/Mohammed-Shbair.**

[3] د. حسين مقداد عبد اللطيف، دور الضبط الإداري في الحد من مخاطر الفضاء الإلكتروني في مصر وفرنسا، مجلة العلوم القانونية والاقتصادية، العدد الأول، السنة الخامسة والستون، كلية الحقوق، جامعة عين شمس، يناير 2023م، ص 671.

[4] أ. عماد جاسم حسين الشنكالي، دور الضبط الإداري الإلكتروني في مكافحة الجرائم المعلوماتية، مرجع سابق، ص 11.

[5] د. حسين مقداد عبد اللطيف، دور الضبط الإداري في الحد من مخاطر الفضاء الإلكتروني في مصر وفرنسا، مرجع سابق، ص 672.

ويمكن تعريف الضبط الإداري الإلكتروني بأنه: مجموعة من الإجراءات والتدابير القانونية التي تتخذها السلطات الإدارية باستخدام التقنيات الرقمية المتقدمة، لتنظيم وتقييد الأنشطة الفردية داخل المواقع الإلكترونية، بهدف حماية النظام العام، مع تحقيق التوازن بين حماية المجتمع واحترام حقوق وحريات الأفراد الأساسية.

ويتميز هذا التعريف بالشمولية، حيث يغطي جميع الجوانب المهمة للضبط الإداري الإلكتروني، بما في ذلك الإجراءات والتدابير القانونية والتقنيات المستخدمة والأهداف المرجوة، كما يظهر التفصيل في توضيح أن السلطات الإدارية تستخدم التقنيات الرقمية المتقدمة، مما يشير إلى أن هذه الإجراءات تتضمن أدوات وتقنيات حديثة وفعالة في مكافحة الأنشطة غير القانونية. ويبرز التعريف أيضًا أهمية تحقيق التوازن بين حماية النظام العام واحترام حقوق وحريات الأفراد، وهذا يضمن أن الإجراءات المتخذة لا تنتهك حقوق الأفراد في التعبير والحريات الشخصية. بالإضافة إلى ذلك، يحدد التعريف أن الإجراءات والتدابير المتخذة هي قانونية، مما يضفي شرعية على هذه الأنشطة ويوفر إطارًا قانونيًا واضحًا لعمل السلطات الإدارية. وأخيرًا، يوضح التعريف أن الهدف النهائي هو حماية النظام العام، مما يعطي توجهًا واضحًا للإجراءات المتخذة ويعزز من فهم الغاية من الضبط الإداري الإلكتروني.

ومن خلال التعاريف السابقة، نلاحظ الطبيعة المزدوجة للضبط الإداري الإلكتروني، والتي تجمع بين عنصري القانون والتقنيات الرقمية، في ظل جسامة المخاطر والتهديدات الإلكترونية التي أصبحت ظاهرة اجتماعية متوافقة مع الانتقال للمجتمع الرقمي، على خلاف الضبط الإداري التقليدي الذي يجمع بين عنصري القانون والوسائل المادية متى كان لها مقتضى، مثل التنفيذ بالقوة المادية. ويتميز الضبط الإداري الإلكتروني بفضاء جديد ذي طبيعة افتراضية تفتقر إلى فكرة المكان التقليدي، وهذا ما يجعل الوسائل المادية التقليدية للضبط الإداري قاصرة عن مجابهة مخاطره، سيما في ظل عدم تقيد هذا الفضاء الجديد بالحدود الجغرافية للدول[1].

---

[1] يراجع في نفس المعنى: د. عمر محمد بن يونس، الحقوق والحريات والالتزامات الرقمية في الفقه المقارن، المؤتمر الإقليمي العربي "نحو مجتمع معلومات أكثر عدالة"، خلال الفترة من 13-15 سبتمبر 2004م، عمَّان، الأردن، ص 1؛ د. حسين مقداد عبد اللطيف، دور الضبط الإداري في الحد من مخاطر الفضاء الإلكتروني في مصر وفرنسا، مرجع سابق، ص 672.

وأيضًا:

- Roger Smith and Alan Paterson: Face to Face Legal Services and Their Alternatives: Global Lessons from the Digital Revolution, n. p, n. d, p. and p. ;10

وبناءً على ما تقدم، يمكن القول أن سلطة الضبط الإداري الإلكتروني، والمتمثلة في أنها سلطة مشتقة من ذات السلطة الأصيلة التي تتمتع بها الإدارة تجاه الأنشطة الفردية التقليدية بموجب القوانين المطبقة، هذه السلطة ليست جديدة أو موازية لسابقتها، بل تشكل امتدادًا حقيقيًا لها داخل الواقع الإلكتروني، وتعكس حضور ذات الأطراف والأهداف، ولكن بطابع جديد يعتمد على الوسائل الفنية والبرمجية[1].

الضبط الإداري الإلكتروني إطار شامل يتجاوز حدود التقنية أو الأتمتة:

يجدر بنا القول أن نظرية الضبط الإداري الإلكتروني، والتي تعتمد بالكامل على الوسائل التقنية، لا ينبغي أن يُفهم منه اختزال العملية الضبطية في جوانبها التقنية فقط، بما قد يُعتقد معه أن عملية الضبط الإلكتروني تتم بشكل آلي أو تلقائي دون أي تقدير من السلطة الضبطية الإدارية، ما دام أن وسائلها تقنية ومحيطها رقمي. فهذا الاعتقاد من شأنه تسطيح دور الضبط الإداري في حماية الفضاء الإلكتروني.

وحتى لا يُفهم أن الضبط الإداري الإلكتروني مجرد برمجيات أو تطبيقات إلكترونية تعمل بشكل آلي، وما يستتبعه هذا الاعتقاد من تضييق مفهوم الضبط الإداري الإلكتروني أو التهوين من محاولات التأصيل الفقهي للفكرة، ينبغي التنويه إلى نقطة جوهرية وهي أن الضبط الإداري الإلكتروني ليس مجرد عملية تقنية تتم بشكل آلي عبر حواسب وبرمجيات معدة خصيصًا لهذا الغرض، بل هو إطار قانوني وتقني لتأمين الفضاء الإلكتروني– فضاء العصر الحديث– بما يموج به من مخاطر رقمية تهدد كافة عناصر النظام العام.

وبذلك، فالضبط الإداري الإلكتروني أوسع من مجرد عمليات الأتمتة التي تقوم بها الهيئات والأجهزة الإدارية لحماية بياناتها، مثل جدران الحماية الإلكترونية أو برمجيات الحماية التي تستخدم لتأمين الشبكات والحواسب والحسابات الإلكترونية ضد محاولات الاختراق، سواء كانت بغرض التهكير أو التجسس أو غير ذلك من المخاطر الرقمية[2].

ECLAC: The new digital revolution; From the consumer Internet to the industrial Internet, the fifth Ministerial Conference on the Information Society in Latin America and the Caribbean, held in Mexico City from tov August 2015, p. 27.

[1] أ. محمد سليمان شبير، الإطار القانوني لسلطة الضبط الإداري الإلكتروني في فلسطين، مرجع سابق، ص 314.

[2] لمزيد من التفصيل يراجع: د. حسين مقداد عبد اللطيف، دور الضبط الإداري في الحد من مخاطر الفضاء الإلكتروني في مصر وفرنسا، مرجع سابق، ص 673.

ثانيًا- خصائص الضبط الإداري الإلكتروني:

يتميز الضبط الإداري الإلكتروني بمجموعة من الخصائص والمميزات المتعددة التي تتلاءم مع طبيعة الوظيفة التي يقوم بها، ومن أمثلة هذه المميزات:

1- الصفة الوقائية:

يتميز الضبط الإداري الإلكتروني بالطابع الوقائي، حيث تعني الصفة الوقائية للضبط الإداري الإلكتروني اتخاذ تدابير استباقية لمنع المخاطر المحتملة والتعامل معها قبل أن تتحول إلى مشكلات حقيقية تهدد النظام العام[1]، وتعتمد هذه التدابير بشكل كبير على جمع البيانات وتحليلها باستخدام تقنيات متقدمة مثل الذكاء الاصطناعي والتحليل الضخم للبيانات. ومنها على سبيل المثال، يمكن استخدام أنظمة الذكاء الاصطناعي لتحليل البيانات الجنائية والتنبؤ بالمناطق والأوقات التي قد تشهد نشاطًا إجراميًا مرتفعًا، مما يتيح للشرطة تعزيز وجودها في هذه المناطق لمنع الجرائم قبل وقوعها.

2- التعبير عن سيادة الدولة:

صفة التعبير عن السيادة في الضبط الإداري الإلكتروني، وتعني أن هذا النوع من الضبط يعكس سلطة الدولة وسيادتها على الفضاء الرقمي ضمن حدودها، وتتجلى هذه الصفة في الإجراءات والتدابير التي تتخذها السلطات الإدارية لضمان الامتثال للقوانين الوطنية وحماية النظام العام من التهديدات الإلكترونية. ويعبر الضبط الإداري الإلكتروني عن سيادة الدولة من خلال فرض القواعد واللوائح التي تحكم استخدام الإنترنت والبنية التحتية الرقمية داخل حدودها. ومنها على سبيل المثال، إصدار قانون مكافحة جرائم تقنية المعلومات (القانون رقم 175 لسنة 2018) ليعبر عن سيادة الدولة في الفضاء الرقمي، ويتضمن هذا القانون مجموعة من المواد التي تفرض عقوبات على الجرائم الإلكترونية مثل القرصنة، والاحتيال الإلكتروني، والتنمر الإلكتروني.

3- الصفة الانفرادية:

الصفة الانفرادية هي إحدى الخصائص المهمة للضبط الإداري الإلكتروني، وتعني هذه الخاصية أن القرارات والإجراءات المتعلقة بالضبط الإداري تصدر من قبل السلطات الإدارية

---

[1] يراجع في نفس المعنى: د. ناصر لباد، القانون الإداري: النشاط الإداري، الطبعة الأولى، المكتبة الوطنية الجزائرية، الجزائر، 2004م، ج 2، ص 11.

المختصة وتكون ملزمة دون الحاجة إلى موافقة مسبقة من الجهات الأخرى، وبالتالي لا تلعب إرادة الفرد دورًا في إنتاج هذه الأعمال. وقد تكون هذه القرارات فردية، تتعلق بشخص أو حالة معينة، أو تنظيمية، تنطبق على مجموعة واسعة من الأشخاص أو الحالات[1].

ومن أمثلة القرارات الإدارية الفردية، إزالة محتوى إلكتروني معين من موقع إلكتروني أو منصة اجتماعية؛ لأنه يشكل تهديدًا للأمن العام أو يتضمن تحريضًا على الكراهية، وقد يصدر هذا القرار مباشرة من السلطة الإدارية المختصة مثل هيئة تنظيم الاتصالات. أما من أمثلة القرارات الإدارية التنظيمية، إصدار لوائح تنظيمية تحكم استخدام الإنترنت والشبكات الاجتماعية، مثل قوانين حماية البيانات الشخصية التي تفرض التزامات معينة على الشركات والمؤسسات بشأن كيفية جمع ومعالجة وتخزين البيانات الشخصية للمستخدمين.

4- الصفة التقديرية:

من الخصائص المهمة للضبط الإداري الإلكتروني الصفة التقديرية، وهذه الصفة تعني أن للسلطات الإدارية المرونة والحرية في اتخاذ القرارات التي تراها مناسبة لتحقيق الأهداف المرجوة بناءً على تقديرها للوضع والظروف المحيطة، ويسمح ذلك للسلطات بالتكيف مع التغيرات السريعة في البيئة الرقمية واتخاذ إجراءات تتناسب مع كل حالة على حدة[2]. ومن الأمثلة على ذلك عند اكتشاف تهديد سيبراني جديد، مثل فيروس أو هجوم اختراق، يمكن للسلطات الأمنية أن تقرر بناءً على تقييمها السريع للتهديد، ما إذا كان ينبغي تحذير الجمهور، أو إغلاق الشبكات، أو اتخاذ تدابير أمنية أخرى.

5- التكيّف مع التطورات التكنولوجية:

يتميز الضبط الإداري الإلكتروني بمرونته وقدرته على التكيف مع التطورات السريعة في مجال التكنولوجيا الرقمية، ويتيح هذا للسلطات الإدارية تحديث أدواتها وأساليبها بشكل مستمر لمواكبة التهديدات الجديدة. ومثال ذلك، استخدام تقنيات البلوك تشين لحماية البيانات ومنع التلاعب بها في المعاملات الإلكترونية.

---

[1] يراجع في نفس المعنى: أ. عمر بو قريط، الرقابة القضائية على تدابير الضبط الإداري، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة منتوري، قسنطينة، الجزائر، 2006-2007م، ص 23، بحث منشور على الموقع الآتي: **https://lib.manaraa.com/books** .

[2] يراجع في نفس المعنى: د. جمال مطلق الذنيات، الوجيز في القانون الإداري، الدار العلمية الدولية، عمّان، الأردن، 2003م، ص 112.

6- التوازن بين حماية النظام العام واحترام حقوق وحريات الأفراد:

يحرص الضبط الإداري الإلكتروني على تحقيق التوازن بين حماية النظام العام واحترام حقوق وحريات الأفراد الأساسية، ويجب أن تكون الإجراءات المتخذة قانونية ومتناسبة مع الهدف المراد تحقيقه. ومن الأمثلة على ذلك، فرض قيود على نشر المحتوى العدائي على الإنترنت مع توفير قنوات للإبلاغ عن الانتهاكات وضمان حقوق الأفراد في التعبير الحر.

وإن الإدارة، عند ممارستها لاختصاصها في مجال الضبط الإداري الإلكتروني، يجب ألا تتصرف وفق أهوائها وميولها دون رقابة أو متابعة، بل يجب أن تستند إلى أسباب ومسوغات واقعية. وهذا كله يُعد حماية لحقوق الأفراد وحرياتهم ونشاطهم اليومي عبر الإنترنت.

لذلك، فإن قرارات سلطة الضبط الإداري الإلكتروني، كغيرها من القرارات التقليدية، يجب أن تكون وفقًا للقانون؛ لأنها تمس نشاط وحقوق الأفراد. وعلى الرغم من أهمية هذه السلطة وضرورتها، فإن الرقابة القضائية عليها تظل ذات أهمية بالغة وضرورية لضمان عدم تعسف الإدارة في استخدامها وتجاوز صلاحياتها إلى الإساءة في استخدامها[1].

ثالثًا- تمييز الضبط الإداري الإلكتروني عن غيره من أنظمة الضبط الأخرى:

هناك بعض الفوارق بين الضبط الإداري الإلكتروني وأنظمة الضبط الأخرى المرتبطة به، وتتمثل هذه الفوارق في عدة جوانب منها:

1- التمييز بين الضبط الإداري الإلكتروني والضبط الإداري العادي:

قد سبق القول أن الضبط الإداري الإلكتروني هو: مجموعة من الإجراءات والتدابير القانونية التي تتخذها السلطات الإدارية باستخدام التقنيات الرقمية المتقدمة، لتنظيم وتقييد الأنشطة الفردية داخل المواقع الإلكترونية، بهدف حماية النظام العام، مع تحقيق التوازن بين حماية المجتمع واحترام حقوق وحريات الأفراد الأساسية

وقد عرفنا الضبط الإداري بأنه: مجموعة من الإجراءات والتدابير التي تتخذها السلطات الإدارية، والتي تتمثل في فرض قيود تنظيمية على الحريات العامة والخاصة للأفراد، بهدف الحفاظ على النظام العام بمختلف عناصره. ويتم ذلك من خلال تحقيق التوازن بين مصلحة المجتمع في الحفاظ على النظام العام وبين احترام الحقوق والحريات الأساسية للأفراد.

---

[1] أ. محمد سليمان شبير، الإطار القانوني لسلطة الضبط الإداري الإلكتروني في فلسطين، مرجع سابق، ص 314.

ووفقًا لما تقدم، توجد فوارق رئيسية بين نوعي الضبط الإداري الإلكتروني والضبط الإداري العادي في النطاق والمجال؛ تتمثل في أن الأول يتمحور حول الرقابة والتحكم في الأنشطة التي تتم عبر الإنترنت والواقع الإلكتروني، يشمل ذلك الجرائم السيبرانية مثل التنمر الإلكتروني، وحماية البيانات الشخصية، ومراقبة الأنشطة التجارية الإلكترونية. أما الضبط الإداري العادي فيركز على الأنشطة الواقعية في الحياة اليومية، يشمل ذلك الحفاظ على النظام العام في الأماكن العامة، ومراقبة الأنشطة التجارية التقليدية، وضبط حركة المرور.

كما يختلفان في الأدوات والتقنيات؛ فيعتمد الضبط الإداري الإلكتروني على التكنولوجيا الحديثة مثل الذكاء الاصطناعي، وتحليل البيانات الكبيرة، وتكنولوجيا المعلومات والاتصالات، فتتيح هذه الأدوات للسلطات مراقبة وتحديد الأنشطة المشبوهة بسرعة وكفاءة. في المقابل، يعتمد الضبط الإداري العادي على الأدوات التقليدية مثل الدوريات الشرطية، وكاميرات المراقبة في الأماكن العامة، والتفتيش الميداني.

وأخيرًا، يتميز الضبط الإداري الإلكتروني عن الضبط الإداري العادي في السرعة والكفاءة؛ فالأول يتميز بسرعة الاستجابة والقدرة على التعامل مع كميات كبيرة من البيانات في وقت قصير، ويتيح ذلك للسلطات اتخاذ قرارات سريعة وفعالة للحد من المخاطر الإلكترونية. وعلى النقيض، يكون الضبط الإداري العادي أبطأ في الاستجابة؛ نظرًا لاعتماده على التدخل البشري والميداني، مما قد يتطلب وقتًا أطول لاتخاذ الإجراءات اللازمة.

2- التمييز بين الضبط الإداري الإلكتروني والضبط التشريعي:

يقصد بالضبط التشريعي: إصدار المشرع لقوانين تقيد حريات الأفراد وحقوقهم حفاظًا على النظام العام، وفي ممارسته لهذا الاختصاص، يستند المشرع إلى اختصاصه التشريعي الذي يجد مصدره في الدستور والمبادئ العامة للقانون[1].

وتتمثل أحد الفروق الجوهرية بين الضبط الإلكتروني والضبط التشريعي في طبيعة الجهة المسؤولة؛ فالضبط الإلكتروني يتم بواسطة السلطات الإدارية والتنظيمية التي تعتمد على التكنولوجيا الحديثة لمراقبة الأنشطة الإلكترونية وضمان الامتثال للقوانين واللوائح. بينما الضبط التشريعي يتم بواسطة السلطة التشريعية التي تصدر القوانين التي تنظم وتحدد وتقيد حقوق الأفراد وواجباتهم، مستندة في ذلك إلى الدستور والمبادئ العامة للقانون.

---

[1] د. مازن ليلو راضي، القانون الإداري، منشورات الأكاديمية العربية في الدنمارك، الدنمارك، 2008م، ص57

كما يكمن الاختلاف بينهما في نطاق التطبيق؛ فالضبط الإلكتروني يركز على الأنشطة التي تتم في الفضاء الإلكتروني، مثل حماية البيانات الشخصية، ومكافحة الجرائم السيبرانية، وتنظيم الأنشطة التجارية الإلكترونية. في المقابل، يشمل الضبط التشريعي كافة مجالات الحياة ويحدد الإطار القانوني العام الذي ينظم حقوق الأفراد وحرياتهم، ويشمل ذلك القوانين التي تؤثر على الأنشطة الاقتصادية والاجتماعية والسياسية.. وغيرها.

وأخيرًا، يتميز الضبط الإداري الإلكتروني عن الضبط التشريعي في طبيعة الإجراءات؛ فالضبط الإلكتروني يتخذ شكل قرارات تنظيمية أو فردية تصدر عن السلطات الإدارية، وتكون هذه القرارات قابلة للطعن أمام القضاء الإداري. بينما الضبط التشريعي يتخذ شكل قوانين تشريعية تصدر عن البرلمان أو الهيئة التشريعية المختصة، وتكون هذه القوانين ملزمة للجميع ولا تخضع لرقابة القضاء الإداري، بل يمكن الطعن فيها أمام المحاكم الدستورية إذا تعارضت مع الدستور.

3- التمييز بين الضبط الإداري الإلكتروني والضبط القضائي:

يقصد بالضبط القضائي: الإجراءات التي تتخذها السلطة القضائية للتحري عن الجرائم بعد وقوعها، والبحث عن مرتكبيها، تمهيدًا للقبض عليهم، وجمع الأدلة اللازمة للتحقيق معهم ومحاكمتهم وإنزال العقوبة بحقهم[1].

ويتمثل أحد أوجه الاختلاف بين الضبط الإداري الإلكتروني والضبط القضائي في طبيعة الهدف والوظيفة؛ فالضبط الإداري الإلكتروني يهدف إلى الوقاية من الجرائم والمخالفات عبر الإنترنت ومنع حدوثها، من خلال مراقبة الأنشطة الإلكترونية وحماية البيانات الشخصية، وتطبيق القوانين التنظيمية. على النقيض، يهدف الضبط القضائي إلى التعامل مع الجرائم بعد وقوعها، وذلك بالتحري والبحث عن مرتكبيها، وجمع الأدلة اللازمة لتقديمهم للعدالة ومحاكمتهم وإنزال العقوبة بحقهم[2].

كما يختلف الضبط الإداري الإلكتروني عن الضبط القضائي في الجهة المسؤولة عن التنفيذ؛ فالضبط الإداري الإلكتروني يتم بواسطة السلطات الإدارية والتنظيمية التي تستخدم

---

[1] د. مازن ليلو راضي، القانون الإداري، مرجع سابق، ص 58.

[2] للمزيد من التفاصيل يراجع:

- Lagazette.fr: La Police Administrative, Fiche n° 3, publié à l'adresse https://**www.lagazettedescommunes.com/71608/fiche-n%cb02-2%b-3-la-**.

التكنولوجيا الحديثة لمراقبة الأنشطة الإلكترونية واتخاذ التدابير الوقائية. أما الضبط القضائي، فيتم تنفيذه بواسطة السلطة القضائية التي تتولى التحقيق في الجرائم بعد وقوعها، والبحث عن الأدلة وإجراء المحاكمات لضمان تحقيق العدالة وتطبيق القانون.

وأخيرًا، يتابين الضبط الإداري الإلكتروني بطبيعة إجراءاته التي تصدر في شكل قرارات تنظيمية أو فردية تخضع لرقابة القضاء الإداري إلغاءً وتعويضًا. أما الضبط القضائي، فإنه يصدر في شكل قرارات قضائية لا تخضع لرقابة القضاء الإداري، بل تخضع لسلطات القضاء العادي محل النظر[1].

الفرع الثاني

هيئات الضبط الإداري الإلكتروني

نظرًا لتأثير ظهور الفضاء المعلوماتي الكبير على أحكام نظرية الضبط الإداري التقليدية، قامت الهيئات التشريعية في مختلف الدول بإنشاء العديد من الهيئات والأجهزة الفنية المتخصصة لإدارة مختلف جوانب الفضاء المعلوماتي. بالإضافة إلى ذلك، ظهرت جهات فاعلة جديدة في هذا المجال التقني– حيث أصبحت الكيانات الخاصة الكبرى مسؤولة عن إدارة الجزء الأكبر من هذا الفضاء وفقًا لاستراتيجياتها الخاصة. وقد أدى ذلك إلى تطور مفهوم الضبط الإداري من النواحي العضوية والوظيفية؛ نظرًا لتحكم هذه الكيانات في صياغة العديد من معايير الوصول إلى هذا الفضاء، فضلًا عن أن الطبيعة الخاصة لهذا الفضاء صعبت مهمة سلطة الضبط في الحفاظ على النظام العام.

---

[1] اتجه القضاء في فرنسا نحو تقرير عدم مسؤولية الدولة عن أعمال السلطة القضائية، ومنها إجراءات الضبط الإداري، يراجع:

- **De laubadere– Traite da droit administrative– p.591.**

في حين يعتبر القضاء الإداري المصري أعمال الضبط القضائي أعمال قضائية تخضع لسلطات القضاء العادي.

- يراجع في هذا الشأن: د. سليمان محمد الطماوي، القضاء الإداري: قضاء التعويض وطرق الطعن في الأحكام– دراسة مقارنة، دار الفكر العربي للطباعة والنشر، القاهرة، 1986م، ص 61؛ د. رمزي طه الشاعر، المسؤولية عن أعمال السلطة القضائية، مجلة العلوم القانونية والاقتصادية، المجلد (18)، العدد (2)، كلية الحقوق، جامعة عين شمس، يوليو 1976م، ص 145؛ د. مازن ليلو راضي، القانون الإداري، مرجع سابق، ص 58.

ووفقًا للتفرقة التقليدية بين نوعي الضبط الإداري– الضبط الإداري العام والضبط الإداري الخاص، تنقسم هيئات الضبط الإداري الإلكتروني إلى هيئات الضبط الإداري العام وهيئات الضبط الإداري الخاص:

أولًا– هيئات الضبط الإداري الإلكتروني العام:

يقصد بالضبط الإداري الإلكتروني العام[1]: الإجراءات التي تمارسها السلطات الإدارية بموجب الاختصاصات المخولة إليها، سواء على مستوى الدولة بأكملها أم على مستوى إحدى وحداتها الإقليمية. ويمارس الضبط الإداري في الحالة الأولى أعضاء السلطة المركزية، بينما يمارسه في الحالة الثانية رؤساء الوحدات المحلية ومجالسها، وذلك ضمن حدود القوانين والأنظمة التي تحدد الإجراءات وسلطات الضبط الإداري العام[2].

ويأتي في مقدمة هيئات الضبط الإداري الإلكتروني العام في النظام الفرنسي، رئيس الدولة– كونه المنوط بالسهر على ضمان الامتثال للدستور، والسير المنتظم للسلطات العامة، واستمرارية الدولة، واستقلال الوطن وسلامة أراضيه، وذلك وفقًا للمادة الخامسة من دستور عام 1958م[3]. كما يأتي رئيس الوزراء– باعتباره الموجه لعمل الحكومة، والمسؤول عن الدفاع الوطني، ومتابعة

---

[1] وفقًا لما تنص عليه المادة 2212/2 من التقنين العام للسلطات المحلية الفرنسي رقم 142 لسنة 1996م – المعدلة بالقانون رقم 1545 لسنة 2014م الصادر في 20 ديسمبر 2014م، والذي يدور هذا القانون حول أربعة محاور رئيسة، هي: الأمن العام، والذي يرادف مفهوم السلامة العامة (– la sécurité publique synonyme ici de sûreté publique)، والصحة العامة (la salubrité publique)، والسكينة العامة (la tranquillité publique)، والأخلاق العامة بمفهومها الواسع (la moralité publique au sens large) الذي يتضمن معنى الكرامة الإنسانية واحترامها (le respect de la dignité de la personne humaine).

وتنص المادة الثالثة من قانون هيئة الشرطة المصري رقم 109 لسنة 1971، المستبدلة بالقانون رقم 25 لسنة 2012، على أنه: "تختص هيئة الشرطة بالمحافظة على النظام والأمن العام والآداب، وبحماية الأرواح والأعراض والأموال، وعلى الأخص منع الجرائم وضبطها. كما تختص بكفالة الطمأنينة والأمن للمواطنين في كافة المجالات وتنفيذ ما تفرضه عليها القوانين واللوائح من واجبات".

[2] د. ماجد راغب الحلو، القانون الإداري، دار المطبوعات الجامعية، الإسكندرية، 2000م، ص 473.

[3] ARTICLE 5 de la Constitution du 4 octobre 1958: "Le Président de la République veille au respect de la Constitution. Il assure, par son arbitrage, le fonctionnement régulier des pouvoirs publics ainsi que la continuité de l'État. Il est le garant de l'indépendance nationale, de l'intégrité du territoire et du respect des traités.

ARTICLE 6.

تنفيذ القوانين، والممارس للسلطة الرقابية على أعمال الحكومة، وفقًا للمادة (21) من ذات الدستور[1]. ويشمل ذلك أيضًا وزير الاتصالات- إذ ينوب عن الدولة في ممارسة الوظيفة التنظيمية لقطاع الاتصالات الإلكترونية، بالتعاون مع هيئة تنظيم الاتصالات الإلكترونية والخدمات البريدية وتوزيع الصحف، وفقًا للمادة (32-1) من قانون البريد والاتصالات الإلكترونية، المعدل بالمرسوم رقم 650 لسنة 2021م.

وعلى المستوى المحلي، توجد السلطات المحلية بمستوياتها المختلفة وفقًا للمادة 2211/1 من التقنين العام للسلطات المحلية، المعدلة بالمرسوم رقم 351 لسنة 2012 الصادر في 12 مارس 2012، والتي تنص على أنه: "يساهم رئيس البلدية في سياسة منع الجريمة وفقًا للشروط المنصوص عليها في القسم الأول من الفصل الثاني من الباب الثالث من الكتاب الأول من قانون الأمن الداخلي"[2].

وقد أجمل المشرع العادي المعنى المتقدم في نص المادة الأولى من القانون رقم 1062 لسنة 2001 بشأن الأمن اليومي، الصادر في 15 نوفمبر 2001[3]، والتي تنص على أنه: "يُعتبر الأمن حقًا أساسيًا وشرطًا أساسيًا لممارسة الحريات والحد من عدم المساواة. وعلى هذا الأساس، يتعين على الدولة حماية الأشخاص وممتلكاتهم وامتيازات مواطنتهم، والدفاع عن مؤسساتهم ومصالحهم الوطنية، واحترام القانون، وحفظ الأمن والنظام العام في جميع أنحاء أراضي الجمهورية. وللممثلين عن الدولة والسلطات المحلية والمؤسسات العامة للتعاون بين البلديات أن يشاركوا أيضًا في تنفيذ السياسات الأمنية"[4].

---

(1) ARTICLE 21 de la Constitution du 4 octobre 1958: "Le Premier ministre dirige l'action du Gouvernement. Il est responsable de la défense nationale. Il assure l'exécution des lois. Sous réserve des dispositions de l'article 13, il exerce le pouvoir réglementaire et nomme aux emplois civils et militaires.

(2) Article L2211-1 du Code général des collectivités territoriales; Modifié par Ordonnance n°-2012-351 du 12 mars 2012 art. 7: "Le maire concourt à la politique de prévention de la délinquance dans les conditions prévues à la section 1 du chapitre II du titre III du livre Ier du code de la sécurité intérieure".

(3) LOI 1062-2001 du 15 novembre 2001 relative à la sécurité quotidienne, JORF n°266 du 16 novembre 2001Texte n° 1;

https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000000222052.

(4) Article 1er du LOI 1062-2001 du 15 novembre 2001 relative à la sécurité quotidienne: L'article 1er de la loi no 75-95 du 21 janvier 1995 d'orientation et de

وفي مصر، تتمثل هيئات الضبط الإداري الإلكتروني العام في رئيس الجمهورية– باعتباره رئيس الدولة ورئيس السلطة التنفيذية، الذي يرعى مصالح الشعب ويحافظ على استقلال الوطن ووحدة أراضيه وسلامتها، وذلك وفقًا للمادة 139 من دستور عام 2014. كما تشمل رئيس مجلس الوزراء– باعتباره المسؤول، بعد موافقة مجلس الوزراء، عن إصدار لوائح الضبط، وفقًا للمادة 172 من الدستور ذاته. وتضم أيضًا هيئة الشرطة، المنوطة بكفالة الطمأنينة والأمن للمواطنين، والسهر على حفظ النظام العام والآداب العامة، واحترام حقوق الإنسان وحرياته الأساسية، وفقًا للمادة 206 من الدستور[1]. وأخيرًا، تشمل مديري الأمن بالمحافظات[2]، بمعاونة

---

programmation relative à la sécurité est ainsi rédigé: «Art. 1er. – La sécurité est un droit fondamental. Elle est une condition de l'exercice des libertés et de la réduction des inégalités. “A ce titre, elle est un devoir pour l'Etat, qui veille, sur l'ensemble du territoire de la République, à la protection des personnes, de leurs biens et des prérogatives de leur citoyenneté, à la défense de leurs institutions et des intérêts nationaux, au respect des lois, au maintien de la paix et de l'ordre publics”.

“L'Etat associe, dans le cadre des contrats locaux de sécurité, les collectivités territoriales et les établissements publics de coopération intercommunale, qui participent également à la politique de sécurité. D'autres personnes, morales et privées, et notamment les associations, les bailleurs sociaux et les entreprises de transport, peuvent concourir à l'élaboration et à la mise en oeuvre de ces contrats"

[1] يراجع أيضًا: د. محمد أنس جعفر، عبد المجيد عبد الحفيظ سليمان، أصول القانون الإداري، دار النهضة العربية، القاهرة، 2004م، ص 319.

[2] كان هذا الاختصاص معقودًا للمحافظين، ثم أوكل إلى مديري الأمن، وذلك على النحو الذي ورد في حكم المحكمة الإدارية العليا بأن: "ومن حيث إن المادة السادسة من قانون نظام الإدارة المحلية رقم 124 لسنة 1960، الذي صدر القرار المطعون فيه في ظله، تنص على أن يكون المحافظ ممثلًا للسلطة التنفيذية في دائرة اختصاصه، ويتولى الإشراف على تنفيذ السياسة العامة للدولة وعلى فروع الوزارات في المحافظة وعلى موظفيها، كما يعتبر الرئيس المحلي لهم، ويجوز لكل وزير أن يعهد إلى المحافظ ببعض اختصاصاته بقرار منه، وعلى المحافظ أن يبلغ ملاحظاته إلى الوزراء المختصين في كل ما يتعلق بشؤون المحافظة. وعلى هذا يكون المحافظ بوصفه ممثل السلطة التنفيذية للدولة في نطاق المحافظة المسؤول الأول عن تنفيذ السياسة العامة للدولة في دائرة المحافظة وعن تنفيذ القوانين واللوائح والقرارات الوزارية فيها.

واستنادًا إلى ذلك، أصبح المحافظ في نطاق ولاية الضبط الإداري الوارث الطبيعي لاختصاصات المديرين والمحافظين المنصوص عليها في القوانين، ما دام قد نيط به تنفيذ القوانين واللوائح والقرارات الوزارية. وإذ كان من أهم واجبات هؤلاء المحافظين في هذا المجال اختصاصهم بالمحافظة على الأمن بوصفهم من أعضاء هيئة الشرطة طبقًا لنص المادة الثالثة من القانون رقم 234 لسنة 1955 بنظام هيئة الشرطة، والتي تنص على أنه:

المحافظين، حيث إن الأخيرين يمثلون السلطة التنفيذية ويشرفون على تنفيذ السياسة العامة للدولة، فضلًا عن مسؤوليتهم عن الأمن والأخلاق والقيم العامة بالمحافظات، وذلك وفقًا للمادة 26 من قانون الإدارة المحلية رقم 43 لسنة 1979[1].

وبناءً على ما تقدم، نخلص إلى أن هيئات الضبط الإداري العام وفقًا للنظرية التقليدية للضبط الإداري تدخل في المفهوم العام لسلطة الضبط الإداري الإلكتروني؛ باعتبارها صاحبة

"تختص هيئة البوليس بالمحافظة على النظام والأمن العام وعلى الأخص منع الجرائم وضبطها وحماية الأرواح والأعراض والأموال وتنفيذ ما تفرضه عليها القوانين واللوائح من تكاليف".

غير أنه سرعان ما انتقل هذا الاختصاص بعد صدور قانون الإدارة المحلية المشار إليه إلى مديري الأمن بالمحافظات، حيث عدلت في 1960/7/19 المادة الثالثة من قانون نظام الشرطة المذكور بالقانون رقم 257 لسنة 1960، إذ نص هذا القانون في مادته الأولى على أنه: يُستبدل بلفظي "المحافظين والمديرين" الوارد ذكرهما بالقانون رقم 234 لسنة 1955 بنظام هيئة الشرطة والقوانين المعدلة له لفظ "مديرو أمن بالمحافظات". وعلى ذلك، أصبحت تدابير الضبط الضرورية في مجال المحافظة على النظام والأمن العام من اختصاص مديري الأمن بالمحافظات بصفة أصلية، يتخذونها تحت إشراف وزير الداخلية المباشر. ومن ثم، لم يعد للمحافظ بعد إذ سلب المشرع اختصاصه على الوجه المتقدم سلطة إصدار تدابير الضبط الفردية في هذا المجال، وذلك اعتبارًا بأن مهمة الأمن، حسبما كشفت عنه المذكرة الإيضاحية لقانون الإدارة المحلية، مهمة قومية ارتأى القانون أن يعهد بها كلها إلى الإدارة المركزية.

ومما يؤكد هذا النظر، التعديل الذي أدخله القانون رقم 151 لسنة 1961 على المادة السادسة من قانون الإدارة المحلية، إذ نصت تلك المادة في صورتها المعدلة على أن يعتبر المحافظ مسؤولًا عن الأمن والأخلاق العامة في المحافظة ويرتبط في ذلك ارتباطًا مباشرًا بوزير الداخلية الذي يصدر القرارات اللازمة في هذا الشأن. وواضح من هذا التعديل أن المشرع قصد إلى أن تكون السلطة في هذا الخصوص، حسبما سلف البيان، سلطة مركزية يمارسها وزير الداخلية".

- حكم المحكمة الإدارية العليا، الطعن رقم 465 لسنة 11 ق. ع، جلسة 2 ديسمبر 1967، المكتب الفني لمجلس الدولة، مجموعة المبادئ القانونية التي قررتها المحكمة الإدارية العليا، السنة الثالثة عشرة، العدد الأول من أول أكتوبر سنة 1967 إلى منتصف فبراير 1968، ص 179.

[1] تنص المادة 26 من قانون الإدارة المحلية، المعدلة بالقانون رقم 50 لسنة 1981، ثم بالقانون رقم 145 لسنة 1988، على أنه: "يعتبر المحافظ ممثلًا للسلطة التنفيذية في المحافظة، ويشرف على تنفيذ السياسة العامة للدولة وعلى مرافق الخدمات والإنتاج في نطاق المحافظة. ويكون مسؤولًا عن كفالة الأمن الغذائي ورفع كفاءة الإنتاج الزراعي والصناعي والنهوض به، وله أن يتخذ كافة الإجراءات الكفيلة بتحقيق ذلك في حدود القوانين واللوائح. كما يكون مسؤولًا عن الأمن والأخلاق والقيم العامة في المحافظة، يعاونه في ذلك مدير الأمن في إطار السياسة التي يضعها وزير الداخلية، وعلى مدير الأمن أن يبحث مع المحافظ الخطط الخاصة بالحفاظ على أمن المحافظة لاعتمادها، ويلتزم مدير الأمن بإخطار المحافظ فورًا بالحوادث ذات الأهمية الخاصة لاتخاذ التدابير اللازمة في هذا الشأن بالاتفاق بينهما".

الاختصاص العام بمباشرة سلطة الضبط الإداري. ويباشر هؤلاء الأشخاص سلطتهم الضبطية في تنظيم الفضاء المعلوماتي بناءً على ما ترفعه هيئات الضبط الإداري الإلكتروني من تقارير وتوصيات، وذلك بالطبع في الحالات التي يتجاوز فيها الخطر الذي يهدد النظام العام حدود الصلاحيات المخولة لهذه الأخيرة؛ كأن يتداخل مفهوم الخطر الرقمي مع مفهوم الخطر الذي يهدد سائر إقليم الدولة أو جزءًا منه[1].

ويثور هنا تساؤل هام مفاده: هل يجوز لهيئات الضبط الإداري العام أن تباشر الصلاحيات المخولة لهيئات الضبط الإداري الخاص؟

أجاب بعض الفقه الفرنسي على هذا التساؤل بالقول إن الاتجاه القضائي لمجلس الدولة الفرنسي ليس واضحًا تمامًا في هذا الصدد. ومع ذلك، يمكن الاستنتاج من بعض الأحكام أنه لا يوجد ما يمنع من تدخل هيئات الضبط الإداري العام متى كانت الظروف والملابسات تستدعي ذلك. وهذا يعني أنه في حال وجود ظرف استثنائي يقتضي تدخلًا عاجلًا من المستويات العليا للإدارة الضبطية في الدولة، أو في حال عدم كفاية إجراءات الضبط الإداري الخاص لتجنب المخاطر التي تهدد النظام العام، يمكن للضبط الإداري العام التدخل[2].

وكمثال على ذلك، يمكن الإشارة إلى قرار قطع خدمات الاتصالات والرسائل القصيرة (SMS) عن الهواتف المحمولة وخدمات الإنترنت، والذي اشتهر إعلاميًا بقضية قطع الاتصالات أثناء الثورة. فيُعتبر هذا القرار صادرًا عن إحدى هيئات الضبط العام، حيث أصدرته اللجنة الوزارية المكونة من رئيس الوزراء كرئيس، وعضوية وزراء الدفاع، والداخلية، والخارجية، والإعلام، والاتصالات، ورئيس المخابرات العامة، وأمين عام مجلس الوزراء. كما يمكن القول بأن مفهوم الخطر الرقمي الذي يهدد النظام العام قد تماهى مع مفهوم الخطر الذي يهدد كامل إقليم الدولة تارة، وجزءًا منها تارة أخرى، وذلك وفقًا لما انتهت إليه المحكمة الإدارية العليا في حكمها الشهير في هذا الشأن[3].

---

[1] يراجع: د. حسين مقداد عبد اللطيف، دور الضبط الإداري في الحد من مخاطر الفضاء الإلكتروني في مصر وفرنسا، مرجع سابق، ص 707.

[2] Thomas Chevandier et Autres: 50 Questions.. Les polices adminis-tratives, Cahier détachable, No 331, Le Courrier des maires, Février 2019 .p. 6.

[3] يراجع: د. حسين مقداد عبد اللطيف، دور الضبط الإداري في الحد من مخاطر الفضاء الإلكتروني في مصر وفرنسا، مرجع سابق، ص 708.

ثانيًا- هيئات الضبط الإداري الإلكتروني الخاص:

يقصد بهيئات الضبط الإداري الإلكتروني الخاص: تلك الجهات أو المؤسسات الحكومية المخولة قانونيًا بتنظيم ومراقبة الأنشطة الإلكترونية ضمن نطاق محدد لضمان الامتثال للقوانين واللوائح ذات الصلة. وتتعامل هذه الهيئات مع القضايا المتعلقة بالأمن السيبراني، وحماية البيانات الشخصية، ومكافحة الجرائم الإلكترونية، وضمان سلامة واستقرار البنية التحتية الرقمية. وتشمل مهامها إصدار التراخيص، وإجراء التحقيقات، وفرض العقوبات، والتنسيق مع الهيئات الأخرى على المستوى الوطني والدولي. وتعمل هذه الهيئات ضمن إطار قانوني محدد يهدف إلى حماية النظام العام والأمن القومي في المجال الرقمي، مع مراعاة الحقوق والحريات الأساسية للمستخدمين.

ومن أمثلة هيئات الضبط الإداري الإلكتروني الخاص في فرنسا، الوكالة الوطنية لأمن نظم المعلومات (ANSSI)، وتم إنشاء هذه الهيئة بموجب المرسوم رقم 2009-834 الصادر في 7 يوليو 2009. وتعمل هذه الوكالة تحت إشراف الأمانة العامة للدفاع والأمن الوطني (SGDSN)، وتتولى مجموعة من المهام الرئيسية لضمان حماية المعلومات الحساسة، فتشمل هذه المهام تحديد وتطبيق القواعد الأمنية الفنية والتنظيمية، والإبلاغ عن الحوادث الأمنية من قبل المشغلين الوطنيين الأساسيين، وإجراء عمليات التفتيش للتأكد من الالتزام بالقواعد الأمنية. كما تتولى إدارة الأزمات عبر اتخاذ التدابير اللازمة وفقًا لخطة إدارة الأزمات المعتمدة، وتشجع التعاون بين القطاعين العام والخاص لتعزيز مستوى الأمن السيبراني[1].

كما توجد هيئة تنظيم الاتصالات الإلكترونية والخدمات البريدية (ARCEP)، وتم إنشائها بموجب القانون رقم 96-659 الصادر في 26 يوليو 1996. وتم تأسيس ARCEP في البداية تحت اسم "سلطة تنظيم الاتصالات" (Autorité de Régulation des Télécommunications أو ART) وبدأت مهامها في 5 يناير 1997، وتوسعت مهامها لاحقًا لتشمل تنظيم الخدمات البريدية في 21 مايو 2005، وتمت إعادة تسميتها إلى "سلطة تنظيم الاتصالات الإلكترونية والبريد" (ARCEP).

وتتمثل الاختصاصات والمهام الرئيسية لهيئة تنظيم الاتصالات الإلكترونية والخدمات البريدية (ARCEP) في تحديد وتنفيذ اللوائح على مشغلي الاتصالات (المادة L. 37-1 وما يليها من قانون البريد والاتصالات الإلكترونية- CPCE)، وتخصيص موارد الترددات والأرقام

---

[1] لمزيد من التفصيل يراجع الموقع الرسمي للهيئة: **https://www.ssi.gouv.fr**/.

(المادة L. 42-1 وما يليها والمادة L. 44)، ومراقبة التمويل وتقديم الخدمة الشاملة (المادة L. 35 وما يليها من CPCE)، وتقديم الخبرة والمشورة للحكومة والبرلمان والهيئات التنظيمية الأخرى (المادة L. 36-10 من CPCE)، وفرض العقوبات على المشغلين غير الممتثلين (المادة L. 36-11 من CPCE)، والتحقيق وتسوية النزاعات بين المشغلين (المادة L. 36-8 من CPCE).

وتم تعديل قانون هيئة تنظيم الاتصالات الإلكترونية والبريد (ARCEP) في فرنسا بموجب المرسوم رقم 2021-650 الصادر في 26 مايو 2021، وجاء هذا المرسوم لتطبيق توجيهات الاتحاد الأوروبي المنصوص عليها في التوجيه (EU) 1972/2018، والمعروف باسم "القانون الأوروبي للاتصالات الإلكترونية".

التعديلات الرئيسية التي أدخلها المرسوم:

- **تعزيز صلاحيات جمع المعلومات:** تم توسيع صلاحيات ARCEP لجمع المعلومات لتشمل اللاعبين في السوق بخلاف المشغلين، مما يسمح لها باستفسار الجهات النشطة في القطاعات ذات الصلة بالاتصالات الإلكترونية.
- **تنظيم التزامات الوصول والاستثمار المشترك:** المرسوم يسمح للمشغلين الذين تم تحديدهم على أنهم يتمتعون بقدرة سوقية كبيرة بتقديم التزامات وصول أو استثمار مشترك يمكن لـ ARCEP جعلها ملزمة قانونًا.
- **تشجيع الوصول الشامل إلى الشبكات عالية السرعة:** تم تعزيز قدرة ARCEP على ضمان الوصول الشامل لشبكات الاتصال الفائق السرعة في جميع أنحاء فرنسا، بما في ذلك المناطق النائية.
- **تنظيم مقدمي خدمات الاتصالات الجديدة (OTT):** المرسوم يتيح لـ ARCEP تنظيم مقدمي خدمات الاتصال الفوري والاتصال عبر الإنترنت (OTT) الجدد[1].

وتوجد أيضًا الهيئة الوطنية للمعلوماتية والحريات (CNIL)، وتم إنشاؤها بموجب القانون رقم 78-17 الصادر في 6 يناير 1978، والمعروف باسم "قانون المعلوماتية والحريات". وتتمثل اختصاصات اللجنة الوطنية للمعلوماتية والحريات (CNIL) في ضمان جمع ومعالجة البيانات الشخصية وفقًا للقوانين لحماية الخصوصية، وتنظيم العمليات الإلكترونية بما في ذلك مراقبة الامتثال في مجالات مثل التسويق الإلكتروني وتخزين البيانات، والتحقيق وفرض العقوبات على

[1] للمزيد من التفصيل يراجع الموقع الرسمي للهيئة: **https://en.arcep.fr/arcep.htm**.

منتهكي قوانين حماية البيانات، وإصدار التراخيص للشركات التي تتعامل مع البيانات الحساسة، وتقديم الإرشادات والتوجيهات للشركات والأفراد حول الامتثال للقوانين المتعلقة بحماية البيانات.

وتم تعديل قانون اللجنة الوطنية للمعلوماتية والحريات (CNIL) بموجب القانون رقم 2004-801 الصادر في 6 أغسطس 2004، وقد جاء هذا التعديل لتنفيذ توجيه الاتحاد الأوروبي EC/46/95 بشأن حماية البيانات الشخصية، وتضمنت التعديلات تعزيز حماية البيانات الشخصية بإدخال تدابير صارمة لضمان حماية البيانات عند معالجتها إلكترونيًا، وتنظيم عمليات معالجة البيانات بوضع قواعد وإجراءات تركز على الشفافية والمساءلة، وتوسيع صلاحيات اللجنة الوطنية للمعلوماتية والحريات (CNIL) للتحقيق وفرض العقوبات على المخالفين، ومواءمة القانون مع التوجيهات الأوروبية لضمان توافق التشريعات الفرنسية مع قوانين الاتحاد الأوروبي بشأن حماية البيانات[1].

أما فيما يتعلق بالوضع في مصر، وكنتيجة لتقدمية المشرع العادي ومن قبله المشرع الدستوري، في تنظيم العديد من جوانب الفضاء المعلوماتي، فقد تعددت جهات وهيئات الضبط الإداري الإلكتروني الخاص، ويأتي في مقدمة هذه الهيئات، الجهاز القومي لتنظيم الاتصالات. وتم تنظيم عمل الجهاز القومي لتنظيم الاتصالات (NTRA) بموجب قانون تنظيم الاتصالات رقم 10 لسنة 2003.

وتتمثل اختصاصات الجهاز القومي لتنظيم الاتصالات (NTRA) في تنظيم القطاع من خلال إصدار التراخيص وتصاريح التشغيل لشبكات وخدمات الاتصالات وضمان التزام المشغلين باللوائح والقوانين المعمول بها، وإدارة الطيف الترددي بتخصيص الترددات اللاسلكية وإدارتها بما يضمن استخدامها بكفاءة وتجنب التداخل الضار. كما تشمل الاختصاصات ضمان الجودة والكفاءة عبر مراقبة جودة وكفاءة خدمات الاتصالات لتلبية احتياجات المستخدمين، وحماية حقوق المستهلكين والتعامل مع شكاواهم، وتعزيز المنافسة بدعم بيئة تنافسية عادلة بين مشغلي الاتصالات لتعزيز الابتكار، وضمان أمن شبكات الاتصالات والمساهمة في حماية الأمن الوطني. وتساعد هذه الاختصاصات في إدارة وتنظيم قطاع الاتصالات بشكل فعال، مما يضمن تقديم خدمات اتصالات عالية الجودة تتوافق مع المعايير الدولية وتلبي احتياجات المستخدمين في جميع أنحاء مصر[2].

---

[1] للمزيد من التفصيل يراجع الموقع الرسمي للهيئة: **https://www.legifrance.gouv.fr/.**

[2] للمزيد من التفصيل يراجع الموقع الرسمي للجهاز القومي لتنظيم الاتصالات: **https://www.tra.gov.eg/ar/.**

ويدخل أيضًا ضمن مفهوم هيئات الضبط الإداري الإلكتروني الخاص في مجال الصحافة والإعلام الرقميين، المجلس الأعلى لتنظيم الإعلام (SCMR)، المنشأ بموجب القانون رقم 180 لسنة 2018 بشأن التنظيم المؤسسي للصحافة والإعلام، ويتولى هذا المجلس تنظيم شؤون الإعلام المسموع والمرئي والرقمي، سواء في الصحافة المطبوعة أو الرقمية أو غيرها، ويسري على الكيانات والمؤسسات والوسائل الصحفية والإعلامية والمواقع الإلكترونية، ويتمتع بالاستقلال الفني والمالي والإداري[1].

وتتمثل اختصاصات المجلس الأعلى لتنظيم الإعلام (SCMR) وفقًا لهذا القانون في إصدار التراخيص للقنوات البصرية، والسمعية، والرقمية، والمنصات الرقمية والأقمار الصناعية، ومراقبة الامتثال للقوانين والمعايير المهنية والأخلاقية وحماية حقوق الجمهور، وحماية الأمن القومي من خلال منع نشر أو بث المحتويات التي تهدد الأمن القومي وفرض الرقابة على وسائل الإعلام والمواقع الإلكترونية عند الضرورة، وتنظيم المحتوى بحظر نشر الأخبار الكاذبة والتحريض على العنف والكراهية، ومراقبة المحتويات التي تنتهك النظام العام والأخلاق، وإدارة الشكاوى المتعلقة بمحتوى وسائل الإعلام واتخاذ الإجراءات المناسبة ضد المخالفين، وتنظيم المواقع الإلكترونية بمنح التراخيص والإشراف على محتواها، بما في ذلك المدونات وحسابات التواصل الاجتماعي التي تتجاوز عدد متابعيها 5000.

ويُضاف إلى هيئات الضبط الإداري الإلكتروني الخاص المذكورة آنفًا، المجلس الأعلى للأمن السيبراني (ESCC)، المُنشأ بقرار رئيس مجلس الوزراء رقم 2259 لسنة 2014، والذي يضم ممثلين عن وزارات الدفاع والداخلية والخارجية والبترول والكهرباء والصحة والموارد المائية والتموين والاتصالات، إضافة إلى جهاز المخابرات العامة والبنك المركزي، وعناصر من ذوي الخبرة في الجهات البحثية والقطاع الخاص.

ومن أهم اختصاصات هذا المجلس، وفقًا لقرار رئيس مجلس الوزراء رقم 1630 لسنة 2016، اعتماد أطر واستراتيجيات وسياسات[2] تأمين البنية التحتية للاتصالات والمعلومات الحرجة لكافة قطاعات الدولة، ووضع المعايير الملزمة لكافة الجهات كحد أدنى لتأمين البنية التحتية الحرجة للاتصالات والمعلومات، وإلزامها بإعداد خطط الطوارئ، ووضع آليات رصد

---

[1] ألغى هذا القانون، القانون رقم 96 لسنة 1996 بشأن تنظيم الصحافة، والقانون رقم 92 لسنة 2016 بإصدار قانون التنظيم المؤسسي للصحافة والإعلام.

[2] أنشأ المجلس الأعلى للأمن السيبراني الاستراتيجية الوطنية للأمن السيبراني (2017–2021)، ثم أنشأ الاسرتيجية الوطنية للأمن السيبراني (2023–2027).

المخاطر والمتابعة الدورية للهجمات السيبرانية، وتوزيع الأدوار على المستوى الوطني، والتعاون والتنسيق إقليميًا ودوليًا مع الجهات ذات الصلة في مجال الأمن السيبراني، وتأمين البنية التحتية الحرجة للاتصالات والمعلومات، وإعداد توصيات بأية تدخلات تشريعية لازمة للتأمين[1].

ويجب التأكيد على أن الهيئات المذكورة أعلاه للضبط الإداري الإلكتروني، سواء كانت عامة أم خاصة، ذُكرت على سبيل المثال لا الحصر، وهناك هيئات فنية أخرى مختصة بتنظيم شؤون مختلفة من شؤون الفضاء المعلوماتي، مما يجعلها جزءًا من مفهوم هيئات الضبط الإداري الإلكتروني. وقد تكون هذه الهيئات منشأة بموجب تشريعات قائمة أو قد تستحدث مستقبلًا وفقًا لتحديثات البنية التشريعية التي تنظم الوصول إلى الفضاء الإلكتروني بمفهومه الواسع، بما يشمل شقيه العضوي والوظيفي.

ويثور هنا تساؤل هام هو: هل يجوز لهيئات الضبط الإداري الخاص أن تباشر بعض المهام المخولة لهيئات الضبط الإداري العام؟

أجاب على هذا التساؤل بعض الفقه المصري[2] بالقول إن الضبط الإداري الخاص يقيمه المشرع بقوانين خاصة لتنظيم بعض أنواع النشاط ويعهد به إلى سلطة إدارية خاصة بقصد تحقيق أهداف محددة، قد تكون ضمن أهداف الضبط الإداري العام، ومع ذلك يعهد بها المشرع إلى سلطة إدارية خاصة لتحقيق تلك الأهداف بفعالية أكبر، مثال ذلك الرقابة على المحلات الخطرة والمضرة بالصحة العامة.

المطلب الثاني

مفهوم التنمر الإلكتروني وأسبابه وآثاره السلبية

تمهيد وتقسيم:

يعد التنمر من أكثر السلوكيات المرضية الخطيرة انتشارًا، خصوصًا بين المراهقين وفي المؤسسات التربوية والتعليمية وكذلك في الجامعات. تقوم هذه الظاهرة على القمع والقهر وشعارها "أنا أضطهدك إذن أنا موجود". ورغم خطورة الظاهرة وآثارها السلبية، إلا أن الجهود المبذولة

---

[1] لمزيد من التفاصيل يراجع الاستراتيجية الوطنية للأمن السيبراني على الموقع الآتي:

- **https://mcit.gov.eg/Upcont/Documents/swf/National_Cybersecurity_Strategy_2023.**

[2] د. ماجد راغب الحلو، القانون الإداري، مرجع سابق، ص 474.

لتعريفها وتحديد معالمها الرئيسية لم تستقر بعد، خاصة وأنها قد شهدت تطورًا وانتقالًا من شكلها التقليدي الذي كان يحدث في ساحات المدارس والمؤسسات إلى الفضاء الافتراضي، مما جعلها أكثر خطورة في صورها الجديدة بسبب ظهور عناصر العلانية والتشهير ونشر الصور المسيئة وغيرها. وسوف نتناول في هذا المطلب التعريف بهذه الظاهرة، وصورها، وأسبابها، وأخطارها، وذلك في فرعين على النحو الآتي:

- **الفرع الأول: مفهوم التنمر الإلكتروني.**
- **الفرع الثاني: أسباب التنمر الإلكتروني وآثاره السلبية.**

الفرع الأول

مفهوم التنمر الإلكتروني

أولًا- تعريف التنمر[1] الإلكتروني:

1- التعريف التشريعي للتنمر الإلكتروني:

أ. تعريف المشرع الفرنسي للتنمر الإلكتروني:

يحتوي قانون العقوبات الفرنسي على عدة نصوص تعاقب على التنمر إذا ارتكب في بيئات متعددة مثل بيئة العمل، أو في إطار الأسرة بين الزوجين أو في اتفاق تضامن مدني. ومع انتشار ظاهرة التنمر خارج هذه الحالات، استدعى ذلك من المشرع الفرنسي إضافة مواد جديدة تعاقب على التنمر بوجه عام.

وقد نُص على هذه الجريمة في قانون العقوبات الفرنسي في المواد من (222-33-2 إلى 222-33-2-2) في الباب الثاني من الكتاب الثاني تحت عنوان: "التحرش المعنوي" (harcèlement moral). ويشير مصطلح "التحرش" (harceler) في اللغة الفرنسية القديمة

---

[1] جاءت كلمة التنمر في اللغة العربية من النمر، فنِمَرَ يَنمُرُ، نَمْرًا، فهو نَمِرٌ وأنمَرُ. وتنمَّر الشخص: غضِبَ وساء خلقه فصار كالنمر الغاضب. وتنمَّر: أي تشبَّه بالنمر في لونه أو طبعه، ويقال: دائمًا أنت متنمِّر. وتنمَّر لمنافسه: تنكَّر له وأوعده. يراجع: د. أحمد مختار عمر، معجم اللغة العربية المعاصرة، الطبعة الأولى، دار عالم الكتب، القاهرة، 2008م، ج 3، ص 2285. إذن يدور المعنى اللغوي للتنمر حول التهديد والتوعد، إذ يُقال "تنمر لفلان" أي عبس وتغير وجهه. وأصل الكلمة من شراسة الخلق، والنمر هو الحيوان المعروف بشراسته واستعداده الدائم للهجوم. ويعكس التنمر السلوكي هذا المعنى، حيث يخرج المتنمر عن نطاق الشرع والعرف، ومخالفة الصواب.

إلى الإساءة في المعاملة والتعذيب أو الإزعاج (malmener et tourmenter)، ويقصد به الخضوع دون توقف لاعتداءات صغيرة ومتكررة وسريعة ومتواصلة.

ولا يقتصر التنمر أو التحرش المعنوي وفق المصطلح الفرنسي على بيئة محددة، بل يمكن أن ينطبق على أي بيئة. فقد ترتكب سلوكيات التنمر في الجامعات، والمدارس، والملاعب الرياضية، وعلاقات العمل، كما قد ترتكب في نطاق الأسرة بين الزوجين أو الخليلين وفق عقد تضامن. وقد يكون المجني عليه في هذه الجريمة أحد معارف الجاني أو غريبًا عنه، ويكثر التنمر في الحالة الأخيرة عبر الإنترنت من خلال وسائل التواصل الاجتماعي[1].

ووفقًا للمادة (222-33-2) من قانون العقوبات، يمكن تعريف التنمر في بيئة العمل بأنه: مضايقة الآخرين من خلال القول أو الفعل المتكرر الذي يكون هدفه أو أثره تدهور ظروف العمل مما يمس بحقوقهم وكرامتهم، أو يؤثر في صحتهم الجسدية أو العقلية، أو يعرض مستقبلهم المهني للخطر.

ويلاحظ على تعريف المشرع الفرنسي للتحرش المعنوي في العمل أنه أخذ بالمفهوم الواسع إلى حد كبير، كما أنه اهتم بالتركيز على آثار التنمر أكثر من تركيزه على أسبابه وعناصره، بالإضافة إلى أنه يحظر فقط تكرار السلوك ولا يعاقب عليه إذا لم يتحقق التكرار.

ولمعاقبة التنمر أو التحرش المعنوي يجب أن يقع بشكل متكرر في بيئة العمل أو بمناسبته، ويكفي لمعاقبة الجاني أن يكون أثر هذا السلوك محتملًا. ويمكن أن يحدث هذا النوع من التنمر من العاملين في بيئة عمل معينة، أو من صاحب مصلحة بمناسبة أداء العمل، وقد يكون الجاني رئيسًا للمجني عليه، ويكون التنمر في هذه الحالة رأسيًا من أعلى إلى أسفل، أو أفقيًا عندما يرتكب من أحد العاملين تجاه زميله في المستوى الوظيفي نفسه، أو عموديًا إلى أعلى عندما يكون الجاني مرؤوسًا لضحيته[2].

وعرف قانون العمل الفرنسي التحرش المعنوي وفقًا لنص المادة (1152-1) بأنه: "لا يجوز لأي موظف أن يتعرض لأعمال متكررة من التحرش الأخلاقي يكون لها هدف أو أثر في تدهور ظروف العمل، مما يخل بحقوقه وكرامته ويضر بصحته البدنية أو العقلية أو بمستقبله المهني".

---

[1] د. حسين بن سعيد الغافري، جريمة التنمر الإلكتروني عبر وسائل التواصل الاجتماعي، مجلة روح القوانين، المجلد 35، العدد 103، كلية الحقوق، جامعة طنطا، يوليو 2023م، ص 1104.

[2] المرجع السابق، ص 1105.

كما قرر المشرع الفرنسي تجريم التنمر بين الأزواج أو الشركاء المرتبطين وفق اتفاق تضامن مدني أو بدون هذا الاتفاق من خلال القانون رقم 769 لسنة 2010 بشأن العنف ضد المرأة. فأضيفت المادة رقم (222-33-2-1) إلى قانون العقوبات لتعريف التنمر في إطار هذه العلاقة بأنه: أقوال أو أفعال متكررة تهدف إلى تدهور ظروف المعيشة مما يمس بالصحة الجسدية أو العقلية للمجني عليه.

ولا يشترط المشرع الفرنسي لاستعمال حكم المادة (222-33-2-1) أن تكون العلاقة بين الجاني وضحيته قائمة، إذ تطبق العقوبات حتى لو كانت الجريمة قد ارتكبت من زوج سابق، أو شريك سابق.

وتبنى المشرع الفرنسي أيضًا في القانون رقم 873 الصادر في 4 أغسطس 2014 بشأن المساواة الفعلية بين المرأة والرجل، مضيفًا المادة رقم (222-33-2-2) إلى قانون العقوبات لتجريم التنمر بشكل عام، دون اشتراط وجود علاقة بين الجاني والضحية.

كما عرف المشرع الفرنسي التنمر في المادة الأولى من القانون رقم 2022-299 الصادر في 2 مارس 2022 الذي يهدف إلى مكافحة التنمر في المدارس والجامعات، بأنه: "لا يجوز لأي طالب أو تلميذ أن يتعرض لأعمال تنمر ناتجة عن أقوال أو تصرفات تُرتكب داخل المؤسسة التعليمية أو في محيط الحياة المدرسية أو الجامعية، وتهدف أو تؤدي إلى المساس بكرامته، أو تضر بصحته الجسدية أو العقلية، أو تؤدي إلى تدهور ظروف تعليمه. ويمكن أن تشكل هذه الأفعال جريمة التنمر المدرسي المنصوص عليها في المادة (222-33-2-3) من قانون العقوبات"[1].

وبناءً على ما تقدم، ينص قانون العقوبات الفرنسي على عقوبات التنمر في بيئات مختلفة مثل العمل والأسرة والعلاقات المدنية. ومع توسع الظاهرة، أضاف المشرع مواد جديدة لمعاقبة التنمر بشكل عام، منها المواد (222-33-2 إلى 222-33-2-2)، كما عاقب القانون على السلوكيات المتكررة التي تهدف إلى تدهور ظروف العمل أو المعيشة وتؤثر على الكرامة

---

[1] Article 1: "Aucun élève ou étudiant ne doit subir de faits de harcèlement résultant de propos ou comportements, commis au sein de l'établissement d'enseignement ou en marge de la vie scolaire ou universitaire et ayant pour objet ou pour effet de porter atteinte à sa dignité, d'altérer sa santé physique ou mentale ou de dégrader ses conditions d'apprentissage. Ces faits peuvent être constitutifs du délit de harcèlement scolaire prévu à l'article 222-33-2-3 du code pénal".

والصحة الجسدية أو العقلية للضحية، سواء في بيئة العمل، أو بين الأزواج، أو في المؤسسات التعليمية. وتظهر هذه التعديلات مدى اهتمام المشرع الفرنسي بحماية الأفراد في جميع البيئات من التنمر والتحرش المعنوي.

ب. تعريف المشرع المصري للتنمر الإلكتروني:

وفقًا للمذكرة الإيضاحية لمشروع القانون بشأن تعديل قانون العقوبات والذي عرف التنمر ونص على عقوبته، فإن هذا التعديل التشريعي جاء لمواجهة ظاهرة التنمر المتنامية والتي تشكل خطرًا على المجتمع وعائقًا أمام تطبيق موجبات الحياة الكريمة للمواطنين. وأشارت المذكرة إلى أن مشروع القانون يتوافق مع المادة (8) من الدستور المصري 2014 التي تقضي بأن يقوم المجتمع على التضامن الاجتماعي وتلتزم الدولة بتحقيق العدالة الاجتماعية وتوفير سبل التكافل الاجتماعي لضمان الحياة الكريمة لجميع المواطنين.

وعرفت المادة 309 مكرر ب من القانون رقم 189 لسنة 2020 التنمر بأنه: "كل قول أو استعراض قوة أو سيطرة للجاني أو استغلال ضعف المجني عليه أو حالة يعتقد الجاني أنها تسيء للمجني عليه مثل الجنس أو العرق أو الدين أو الأوصاف البدنية أو الصحية أو العقلية أو المستوى الاجتماعي، بقصد تخويفه أو وضعه موضع السخرية أو الحط من شأنه أو إقصائه من محيطه الاجتماعي"[1].

ويرى بعض الفقه[2] أن استخدام المشرع المصري لمصطلح "التنمر" في المادة (309 مكرر ب) غير دقيق وكان من الأفضل استخدام مصطلح "التحرش المعنوي" كما في القانون الفرنسي؛ لأنه مصطلح مرن يشمل جميع البيئات من الجامعات والمدارس إلى العلاقات الأسرية والمهنية.

بالإضافة إلى ذلك، أشار– الرأي السابق– إلى أن التعريف المصري للتنمر محل انتقاد لعدم شموله التنمر في بيئة العمل، وهو أمر شائع. كما أثنى على توسيع المشرع المصري لمفهوم التنمر ليشمل الأقوى على الأضعف ولم يقصره على أماكن معينة كغيره من التشريعات.

وبذلك يُعتبر التنمر سلوكًا يمكن أن يحدث في أي مكان، سواء في المنزل أو الأسرة أو المدرسة أو مكان العمل أو على منصات التواصل الاجتماعي والمواقع الإلكترونية وتطبيقات المراسلة. ويمكن أن تصدر هذه الأفعال من فرد أو جماعة، بغض النظر عن العمر، وتستهدف

---

[1] الجريدة الرسمية، العدد 36 مكرر (ب) في 5 سبتمبر سنة 2020م.

[2] د. حسين بن سعيد الغافري، جريمة التنمر الإلكتروني عبر وسائل التواصل الاجتماعي، مرجع سابق، ص 1110.

فردًا أو جماعة أخرى. وبالرغم من صعوبة تعريف التنمر، فإن تدخل المشرع المصري لوضع تعريف له كان ضروريًا وقد وُضعت نقاط محددة لتقديم تعريف شامل ومناسب[1].

وهديًا على ما تقدم، فإن المذكرة الإيضاحية لمشروع تعديل قانون العقوبات المصري، الذي عرف التنمر ونص على عقوبته، جاء لمواجهة ظاهرة التنمر المتنامية والتي تُعد خطرًا على المجتمع وعائقًا أمام تطبيق الحياة الكريمة للمواطنين. وأشارت المذكرة إلى توافق مشروع القانون مع المادة (8) من الدستور المصري 2014، التي تؤكد على التضامن الاجتماعي والعدالة الاجتماعية وتوفير سبل التكافل. وعرفت المادة 309 مكرر ب من القانون رقم 189 لسنة 2020 التنمر بشكل يشمل استعراض القوة أو السيطرة أو استغلال ضعف المجني عليه.

2- التعريف الفقهي للتنمر الإلكتروني:

يعد التنمر الإلكتروني ظاهرة عالمية جديدة نسبيًا تشمل مجموعة متنوعة من السلوكيات، ومع ذلك لم يحظَ التنمر الإلكتروني بتعريف مقبول عالميًا، فلا يوجد إجماع على تعريف دقيق وشامل وموحد له دوليًا أو إقليميًا. ومع ذلك تتفق معظم المفاهيم الحالية على أنه شكل من أشكال التنمر التقليدي يتم ارتكابه من خلال وسائل الإعلام الإلكترونية الحديثة.

ومع ذلك هناك محاولات متعددة لتعريف هذه الظاهرة من قبل الأوساط الأكاديمية؛ فقد عرف علماء الاجتماع التنمر الإلكتروني بأنه: نوع من أنواع الإزعاج المتعمد والمضايقات التي تتم عبر الإنترنت بواسطة شخص أو جماعة من الأفراد، ويتم ذلك من خلال التحرش اللفظي أو الإيذاء النفسي، حيث يستخدم المتنمر الإلكتروني التآمر والتلاعب كوسيلة لإذلال الآخرين واحتقارهم، ووضعهم موضع السخرية من زملائهم أو باقي أفراد المجتمع. وتشمل هذه الأفعال الاستهزاء أو التنابز بالألقاب، والتمييز العرقي والديني، ونشر الشائعات الخبيثة، والتحرش والتهديد باستخدام الوسائط التقنية المعلوماتية الحديثة[2].

كما عرفه بعض من الفقه القانوني بأنه: جريمة عمدية لا يتصور فيها الخطأ تنجم عن إيذاء متعمد ومتكرر يتم باستخدام الوسائل الإلكترونية من أجل النيل بالضحية على مستوى

---

[1] د. كمال سيد عبد الحليم، جريمة التنمر وعقوبتها في الشريعة والقانون، مجلة كلية الشريعة والقانون، العدد الرابع والثلاثون، الإصدار الأول، جامعة الأزهر، فرع أسيوط، يناير 2022م، ص 739.

[2] د. عدنان أبو مصلح، معجم علم الاجتماع، مكتبة العبدلي، عمَّان، الأردن، 2010م، ص 11.

نفسي وجنسي وجسدي بالقول أو بالإشارة أو العلامة من أجل الحط من قدر الضحية وإضعاف شأنه في وسطه الاجتماعي[1].

كما عُرّف بأنه: سلوك عدواني يتم عبر الإنترنت أو وسائل الإعلام الإلكترونية أو الرقمية التي تتاح للمتنمر، والذي يقوم به فرد أو جماعة من خلال الاتصال المتكرر الذي يتضمن رسائل عدائية تهدف لإلحاق الأذى بالآخرين وقد تكون هوية المتنمر مجهولة أو معروفة للضحية[2].

كما يعرف التنمر الإلكتروني أيضًا بأنه: شكل من أشكال العدوان، يعتمد على استخدام وسائل الاتصال الحديثة وتطبيقات الإنترنت (الهواتف المحمولة، والحاسوب المحمول، وكاميرات الفيديو، والبريد الإلكتروني، وصفحات الإنترنت) في نشر منشورات (بوستات) أو تعليقات تسبب الضرر بالآخرين، أو الترويج لأخبار كاذبة، أو إرسال رسائل إلكترونية لإلحاق الضرر المعنوي والمادي بالآخرين[3].

كما عرفه البعض الآخر بأنه: فعل أو سلوك عدواني يتم تنفيذه باستخدام الوسائل الإلكترونية من قبل مجموعة أو فرد بشكل متكرر ومع مرور الوقت ضد ضحية لا يمكنها الدفاع عن نفسها بسهولة[4].

ويمكن تعريف التنمر الإلكتروني بأنه: سلوك عدواني عمدي ومتكرر يُمارَس باستخدام وسائل الإعلام الإلكترونية أو الرقمية، ويُنَفَّذ بواسطة فرد أو مجموعة، وغالبًا ما يتخفى المتنمرون خلف هويات مجهولة أو وهمية. ويهدف هذا السلوك إلى إلحاق الأذى النفسي، أو الجسدي، أو الاجتماعي بالضحية من خلال التحرش اللفظي، والتهديد، والتلاعب، ونشر الشائعات الخبيثة، والتمييز العرقي والديني، والإذلال العلني. ويمكن أن ينتشر تأثير التنمر الإلكتروني بسرعة ويستمر لفترات طويلة، مما يسبب آثارًا نفسية واجتماعية خطيرة على الضحية مثل القلق، والاكتئاب، والعزلة، وتدهور الأداء الأكاديمي أو المهني.

---

[1] د. كمال سيد عبد الحليم، جريمة التنمر وعقوبتها في الشريعة والقانون، مرجع سابق، ص 740.

[2] د. حسين بن سعيد الغافري، جريمة التنمر الإلكتروني عبر وسائل التواصل الاجتماعي، مرجع سابق، ص 1098.

[3] Beran, T., & Li.Q., The relationship between cyberbullying and school bulling, The Journal of Student Wellbeing, 1 (2),2008,p. 17.

[4] د. أحمد محمد عبد الرؤوف المنيفي، التنمر وابتزاز النساء عبر الإنترنت، مركز الكتاب الأكاديمي، القاهرة، 2020م، ص 12.

وبناءً على ما تقدم، يمكن القول أن ظاهرة التنمر الإلكتروني تشترط التكرار خلال مدة معينة، فلا يكفي أن يحدث التنمر مرة واحدة، فيعتمد المتنمر الإلكتروني أساسًا على استغلال نقاط ضعف الضحية لإيقاع الضرر به، ويكمن خطر التنمر الإلكتروني في كونه ظاهرة إجرامية تهدف إلى النيل من شخصية الضحية، وكسر ثقته بنفسه، وتقليص قيمته واعتباره أمام نفسه والآخرين، مما يبرز الخطورة الإجرامية الكامنة في سلوك المتنمر الإلكتروني.

والتنمر الإلكتروني جريمة عمدية تتطلب أن يكون المتنمر قاصدًا إيذاء الضحية، أو تخويفه، أو وضعه موضع السخرية، أو الحط من شأنه، أو إقصائه من محيطه الاجتماعي. ولا تقتصر ظاهرة التنمر الإلكتروني على الهجمات الشخصية ضد الأطفال أو البالغين، بل تشمل أيضًا التحرش الإلكتروني أو المطاردة الإلكترونية عبر المواقع الإلكترونية، والمدونات، وغرف الدردشة، والتعليقات على المنتجات في نطاق التجارة الإلكترونية.

ويشمل التنمر الإلكتروني أيضًا التعليقات الضارة على السلع والخدمات التي تهدف إلى تشويه سمعة المنتجات أو الخدمات، وذلك بنشر تعليقات كاذبة تؤدي إلى انخفاض الطلب عليها. وفي هذا السياق، قضت المحكمة التجارية في باريس بتاريخ 26 يوليو 2011 بإلزام مدير شركة بدفع مبلغ 10,000 يورو كتعويض لاستخدامه كلمات وتعبيرات معيبة بحق مقدم خدمات كان في حالة غضب منه[1]، مما اعتُبر نوعًا من التنمر الإلكتروني من خلال التعليقات الكاذبة والشائعات الإلكترونية بشأن السلع والخدمات.

ثانيًا– التمييز بين التنمر الإلكتروني وبعض المصطلحات المتشابهة معه:

هناك بعض الفوارق بين التنمر الإلكتروني وبعض المصطلحات الأخرى المتشابهة معه أو المرتبطة به، وتتمثل هذه الفوارق في عدة جوانب، منها:

[1] Tribunal de commerce de Paris, 26 Juillet 2011, cite par: Fabrice MATTATIA, Internet et les réseaux sociaux, que dit la loi ? éd., Eyrolles, 2 éme, Paris, 2016, P. 22.

1- التنمر الإلكتروني والتنمر التقليدي:

يعرف التنمر التقليدي بأنه: تكرار مجموعة من الهجمات والمضايقات والسلوكيات مثل السخرية، والتوبيخ، والتهديد بالضرب من قبل شخص يُعرف بالمتنمر تجاه شخص آخر يُعد ضحية؛ وذلك بهدف السيطرة عليه واكتساب القوة التي لا تتحقق إلا بجعل الآخر ضحية[1].

وبذلك، يختلف التنمر الإلكتروني عن التنمر التقليدي في العديد من الجوانب المهمة؛ حيث يتميز الأول باستخدام التكنولوجيا الحديثة ووسائل الاتصال الإلكترونية كوسيلة لارتكاب الأفعال العدائية. فيستغل المتنمر منصات التواصل الاجتماعي، والرسائل النصية، والبريد الإلكتروني، والمدونات لنشر الإساءات والشائعات والتحرش بالضحية، مما يزيد من نطاق وتأثير الأفعال العدائية ويجعلها أكثر انتشارًا وسرعة.

ومن ناحية أخرى، يعتمد التنمر التقليدي على المواجهات المباشرة والتفاعل الشخصي بين المتنمر والضحية، فيحدث هذا النوع من التنمر في بيئات مثل المدارس، وأماكن العمل، والمجتمعات المحلية، حيث يُمارس المتنمر سلوكيات عدوانية مثل العنف الجسدي، والسخرية العلنية، والتوبيخ المباشر. ويقتصر تأثير التنمر التقليدي غالبًا على النطاق المكاني والزمني الذي يحدث فيه، مما يقلل من مدى انتشار الأذى مقارنة بالتنمر الإلكتروني.

ففي دراسة تناولت مقارنة الأثر بين التنمر الإلكتروني والتنمر التقليدي، أكد الطلاب المشاركون في الدراسة أن التنمر الإلكتروني، من خلال استخدام الصور، ومقاطع الفيديو، وغرف الدردشة، له تأثير أكبر مقارنة بالتنمر التقليدي، وأشارت الدراسة إلى أن هذا النوع من التنمر يؤدي إلى زيادة معدلات القلق بين الضحايا، بالإضافة إلى ارتفاع معدلات استخدام الكحوليات والمخدرات بين ضحايا التنمر الإلكتروني الذين تتراوح أعمارهم بين عشرة وخمسة عشر عامًا[2].

علاوة على ذلك، يُعاني ضحايا التنمر الإلكتروني من آثار نفسية واجتماعية أعمق وأطول أمدًا بسبب الطبيعة المستمرة والمُلحّة للهجمات الإلكترونية؛ حيث يمكن أن تستمر الإساءة لفترات

---

(1) ERIC Digest, Banks R.Bullying in school, Washington, DC:U.S.Department of Education and Justice.1997.p.g120-122.

(2) R. M. KOWALSKI & S. P. LIMBER, Psychological, Physical, and Academic correlates of cyberbullying and traditional bullying, Journal of adolescent health, 2013, n°53, PP, 13, 20s.

طويلة وتظل متاحة للعرض على الإنترنت. بينما في التنمر التقليدي، تكون الهجمات محدودة بفترة المواجهة الفعلية، وقد يكون من الممكن للضحية تجنب المتنمر بشكل أسهل.

بالإضافة إلى أن، التنمر الإلكتروني يتميز بصعوبة تحديد هوية المتنمر مقارنة بالتنمر التقليدي، حيث غالبًا ما يتخفى المتنمرون الإلكترونيون خلف هويات مجهولة أو وهمية على الإنترنت، يمكنهم استخدام حسابات مزيفة أو أسماء مستعارة لنشر الإساءة دون الكشف عن هويتهم الحقيقية، مما يزيد من صعوبة تتبعهم ومساءلتهم قانونيًا. في المقابل، يعتمد التنمر التقليدي على المواجهة الشخصية المباشرة بين المتنمر والضحية، مما يجعل من السهل على الضحية ومعلميها أو زملائها التعرف على هوية المتنمر.

وأخيرًا، يختلفان من حيث الإشراف والمراقبة على سلوك المتنمر؛ فالمنتديات الإلكترونية ومواقع التواصل الاجتماعي تفتقر إلى عنصر الإشراف والرقابة، مما يسهل للمتنمر الإلكتروني ارتكاب السلوك الإجرامي المكوّن لهذه الظاهرة. على العكس من ذلك، في حالة التنمر التقليدي، يمكن للمدرسين والمشرفين الحد من أثره على ضحاياه من خلال المراقبة المباشرة. كذلك، فإن معرفة المراهقين للكثير من التقنيات الإلكترونية أكثر من آبائهم أو أولياء أمورهم يجعلهم غير قلقين من اكتشاف أحد والديهم ارتكابهم للتنمر الإلكتروني، وذلك على العكس من التنمر التقليدي. وتشير معظم الدراسات إلى أن الخصائص السيكولوجية تلعب دورًا في تفشي ظاهرة العنف لدى الأفراد المتنمرين، وبالتالي لا ينبغي إغفال هذه العوامل لمواجهة هذه الظاهرة الإجرامية[1].

2- التنمر الإلكتروني والمطاردة الإلكترونية:

تمثل المطاردة الإلكترونية الاستخدام المتكرر للإنترنت أو وسائل الاتصال الحديثة لملاحقة فرد أو جماعة أو مؤسسات، بهدف نشر الاتهامات الكاذبة، والتشهير، والقذف، والتهديد، وسرقة الهوية الشخصية، والتحريض على الجنس، وتخريب الممتلكات، أو جمع معلومات شخصية

[1] للمزيد من التفصيل يراجع: التقرير العالمي لمنظمة الصحة العالمية حول العنف والصحة، جنيف، 2002م؛ د. ياسر محمد اللمعي، المواجهة الجنائية لظاهرة التنمر الإلكتروني في ضوء السياسة التشريعية الحديثة: دراسة تحليلية مقارنة، مجلة روح القوانين، العدد الخامس والتسعون، كلية الحقوق، جامعة طنطا، يوليو 2021م، ص 34.

واستخدامها لمضايقة الضحية وإحراجها أو تهديدها[1]. ويشير مصطلح "المطاردة" إلى مجموعة من التصرفات غير المرغوبة والمتكررة التي يتطفل فيها شخص على آخر.

وتعد المطاردة الإلكترونية جريمة جنائية، وتعالجها الدول في تشريعات مختلفة تقليدية أو مستحدثة لمكافحة المطاردة، والقذف، والتشهير والتحرش ومنها الولايات المتحدة الأمريكية. فقد وضعت الولايات المتحدة الأمريكية عدة معايير قانونية للمطاردة، وبالرجوع إلى "Modal Statutes"، فإن هناك أربعة معايير رئيسية للمطاردة:

- الأول: يجب أن تتضمن المطاردة سلوكًا متكررًا مع مرور الوقت.
- الثاني: يجب أن تنطوي المطاردة على انتهاك الحقوق الشخصية الخاصة للأفراد.
- الثالث: تتطلب المطاردة وجود دليل على التهديد و/أو التخويف؛ وبالتالي، من غير المرجح أن تشكل مجرد مضايقة في شكل مكالمة هاتفية أو رسائل بريد إلكتروني متكررة مطاردة ما لم يكن محتوى تلك الاتصالات أو شكلها أو طبيعتها كافيًا لإثارة الخوف أو الشعور بالرهبة لدى "شخص معقول".
- الرابع: يمكن أن تحدث المطاردة حتى لو كان التهديد أو الخوف الذي يثيره يتعلق بأسرة الشخص المستهدف أو أصدقائه أو حيواناته الأليفة أو ممتلكاته[2].

وبناءً على ما تقدم، يختلف التنمر الإلكتروني عن المطاردة الإلكترونية في عدة جوانب جوهرية؛ فمن حيث التكرار والدوام، يعتمد التنمر الإلكتروني على الأفعال العدائية المتكررة مثل السخرية، والتهديد، ونشر الشائعات الخبيثة، بينما تتسم المطاردة الإلكترونية بالسلوك المستمر والملاحقة طويلة الأمد التي تستهدف الضحية بشكل مستمر ومكثف، مما يعزز حالة الخوف والقلق لديها، فيُعد التكرار في التنمر الإلكتروني عاملًا مهمًا لتمييزه، في حين أن المطاردة الإلكترونية تعتمد على استمرارية السلوك وملاحقة الضحية لفترات زمنية طويلة.

---

[1] BRIAN H.SPITZBERG, GREGORY HOOBLER, Clberstalking and the technologies of interpersonal terrorism new media & society, 2012, (1)4.P.69. see: http://**www-rohan.sdsu.edu/~bsavatar/articles/Cyberstalking- NM&S02.pdf**.

[2] يراجع: د. علي موسى الصبحين، د. محمد فرحان القضاة، سلوك التنمر عند الأطفال والمراهقين (مفهومه- أسبابه- علاجه)، جامعة نايف العربية للعلوم الأمنية، الرياض، 2013م، ص 29؛ د. ندا منعم محمود السيد سلام، مدى كفاية التشريعات لمكافحة جريمة التنمر الإلكتروني: دراسة مقارنة، مجلة البحوث الفقهية والقانونية، العدد الحادي والأربعين، كلية الشريعة والقانون بدمنهور، جامعة الأزهر، إبريل 2023م، ص 742.

أما من ناحية الوسائل المستخدمة، فيرتبط التنمر الإلكتروني بشكل رئيسي بالتفاعلات عبر وسائل التواصل الاجتماعي، والرسائل النصية، والبريد الإلكتروني، حيث تُستخدم هذه الوسائل لنشر الإهانات والشائعات والتلاعب بالضحية. أما المطاردة الإلكترونية، فتشمل بجانب استخدام الوسائل الإلكترونية الحديثة، تركز بشكل أكبر على جمع المعلومات الشخصية للضحية واستخدامها لمضايقتها وتهديدها، كما أن المطاردة الإلكترونية غالبًا ما تتضمن تهديدات صريحة أو ضمنية بإلحاق الأذى بالضحية أو بأحبائها أو ممتلكاتها، مما يعكس عنصر التهديد والتخويف بشكل أكثر وضوحًا مقارنة بالتنمر الإلكتروني.

ومن ناحية أخرى، يختلفان من حيث التأثيرات النفسية والاجتماعية؛ فيسبب التنمر الإلكتروني آثارًا نفسية سلبية مثل القلق، والاكتئاب، والعزلة الاجتماعية نتيجة للإهانات والتلاعب المستمر. في المقابل، تُسبب المطاردة الإلكترونية تأثيرات نفسية أكثر عمقًا وشدة؛ نظرًا لاستمرارية الملاحقة والتهديد المستمر، مما يؤدي إلى شعور الضحية بالخوف الدائم وانتهاك خصوصيتها.

وعليه، تعتبر المطاردة الإلكترونية مستوى أخطر وأعمق من مستويات التنمر الإلكتروني؛ إذ لا تقتصر على الفضاء الإلكتروني فقط، بل تمتد لتتبع الضحايا حتى في منازلهم، مما يؤدي غالبًا إلى اعتداءات وتحرشات جنسية. وبالرغم من أن الإنترنت يوفر فضاءات آمنة وخطوط استغاثة للنساء اللواتي يواجهن العنف، يتم استخدام تقنيات المعلومات والاتصالات من قبل مرتكبي العنف المنزلي، مثل معدات التجسس الإلكتروني وبرامج كشف كلمات السر، لتتبع سلوك الضحايا[1].

3- التنمر الإلكتروني والمضايقة:

عرّفت المحكمة العليا في كاليفورنيا المضايقة بأنها: سلوك يسبب إزعاجًا، ورعبًا، وأسى عاطفيًا كبيرًا لشخص محدد، سواء كان قولًا أم فعلًا، ويتم بصورة مستمرة وملحة وبدون أي سبب مشروع[2].

---

[1] د. ياسر محمد اللمعي، المواجهة الجنائية لظاهرة التنمر الإلكتروني في ضوء السياسة التشريعية الحديثة، مرجع سابق، ص 20.

[2] يراجع: أ. سحر فؤاد مجيد، الجرائم المستحدثة: دراسة معمقة ومقارنة في عدة جرائم، الطبعة الأولى، المركز العربي للنشر والتوزيع، القاهرة، 2019م، ص 125.

وبذلك، يمثلان التنمر والمضايقة سلوكيات مسيئة تستهدف فردًا أو مجموعة أفراد لأسباب دينية، أو عرقية، أو إثنية، أو ثقافية، أو اجتماعية وغيرها. كما يتشابهان من حيث المفهوم؛ إذ يعتمدان على القوة والسيطرة "imbalance of power" مما يؤدي إلى إلحاق الضرر الجسدي والنفسي بالضحية.

إلا أنهما يختلفان في عدة جوانب جوهرية، فمن حيث الاستهداف؛ يركز التنمر الإلكتروني على إلحاق الأذى بشخص معين عبر الوسائل الرقمية، بغض النظر عن خلفيته الشخصية أو الاجتماعية. في المقابل، تستهدف المضايقة فردًا أو مجموعة بناءً على سمات محددة مثل الدين، والعرق، والإثنية، أو الحالة الاجتماعية، مما يجعلها تمييزية بطبيعتها ومرتبطة بانتهاك حقوق الإنسان الأساسية.

كما يختلفان أيضًا من ناحية الاستمرارية والإلحاح؛ فيُعرف التنمر الإلكتروني بالتكرار المستمر للأفعال العدائية مثل نشر الشائعات، والتهديدات، والتحرشات عبر الإنترنت، مما يسبب للضحية أذى نفسيًا وعاطفيًا مستمرًا. أما المضايقة، فتتميز بأنها سلوك ملح ومستمر يتعمد الإزعاج والإرهاب العاطفي والنفسي للضحية، ويكون الهدف منه عادةً هو ترهيب الضحية وإثارة الرعب بداخلها دون مبرر مشروع.

بالإضافة إلى الاختلاف في المعالجة القانونية؛ فيتم التعامل مع التنمر الإلكتروني وفق قوانين خاصة تحمي الأفراد من الأذى الناتج عن الإساءة الرقمية، وتعاقب على الأفعال التي تُرتكب عبر الإنترنت. في المقابل، تُعالج المضايقة تحت إطار قوانين مكافحة التمييز والتحرش، خاصة عندما تستهدف فئات محمية على أساس العرق، أو الدين، أو أي صفة شخصية أخرى.

ثالثًا- صور وأشكال التنمر الإلكتروني:

يتضمن التنمر الإلكتروني العديد من الصور والأشكال التي يقوم المتنمر من خلالها بإلحاق الأذى والضرر المتعمد بالضحية باستخدام الوسائل التكنولوجية الحديثة كمواقع التواصل الاجتماعي، والهواتف الذكية، والحواسيب الإلكترونية وغيرها من الوسائل المتطورة، ومن هذه الصور ما يأتي:

1- التنمر عبر الرسائل النصية أو البريد الإلكتروني:

تتضمن هذه الوسيلة إرسال رسائل نصية تحتوي على عبارات تهديد بالقتل أو بإفشاء الأسرار، أو بث الشائعات، أو ابتزاز الضحية ماديًا أو جنسيًا مقابل عدم تكرار التهديد.

وفي البريد الإلكتروني، يمكن أن يقوم المتنمر بإرسال رسالة تتضمن فيروسًا يستهدف الاستيلاء على بريد الضحية الإلكتروني، مما يتيح له الاطلاع على رسائله وإرسال رسائل مخلة بالحياء أو تهديدية للآخرين باسم الضحية، مما قد يوقع الضحية في حرج ومشكلات اجتماعية. كما قد يلجأ المتنمر إلى إرسال روابط لمواقع إلكترونية مخادعة لافتة للانتباه، وبمجرد دخول الضحية إليها، يتمكن المتنمر من نشر أخبار وصور زائفة وغير لائقة على صفحة الضحية[1].

2- التنمر بنشر الشائعات عبر الإنترنت أو الرسائل النصية:

يقوم المتنمر بنشر الشائعات عن الضحية عبر مواقع التواصل الاجتماعي مثل فيسبوك، أو تويتر، أو إنستجرام، أو المنتديات والمواقع الإلكترونية، أو غرف الدردشة، أو من خلال برامج التراسل الفوري مثل واتساب، وفايبر، وإيمو. ويستهدف هذا السلوك السخرية، أو الاستهزاء، أو التهديد بإلحاق الأذى بالضحية.

3- التنمر بالمضايقات عبر غرف الدردشة ومواقع التواصل الاجتماعي:

نظرًا للإقبال الكبير على هذه المواقع، يستغل المتنمرون ضحاياهم من خلال استدراجهم في محادثات تتطور تدريجيًا لتصبح ذات طبيعة جنسية وتأخذ طابعًا أعمق، ويتفاقم هذا الاستغلال نتيجة لانعدام الرقابة الاجتماعية بين الأطراف المتحادثة[2].

4- التنمر الإلكتروني عبر قرصنة الحسابات وسرقة الهوية الرقمية:

يتضمن سرقة معلومات وبيانات حساب شخص ما لاقتحامه وإرسال رسائل ضارة أو تهديدية. وقد يكشف المتنمرون معلومات شخصية للضحية مثل الاسم الحقيقي وعنوان المنزل أو العمل أو المدرسة على المواقع أو المنتديات الإلكترونية أو غرف الدردشة. كما يمكنهم انتحال الشخصية وإنشاء حسابات وهمية بهدف نشر مواد بأسماء الضحايا لتشويه سمعتهم أو السخرية منهم أو لإذلالهم أو تهديدهم إلكترونيًا، ويقوم البعض بنشر شائعات أو ثرثرة لتحريض الآخرين على كره الضحية والتجمع ضدها.

وفي هذا السياق، قضت المحكمة العليا في لندن في 24 يوليو 2008 بإدانة شخص وإلزامه بدفع تعويضات بمبلغ 22 ألف جنيه إسترليني، لإنشائه حسابًا غير صحيح على فيسبوك

---

[1] د. عمرو محمد محمد درويش، د. أحمد حسن محمد الليثي، فاعلية بيئة تعلم معرفي سلوكي قائمة على المفضلات الاجتماعية في تنمية استراتيجيات مواجهة التنمر الإلكتروني لطلاب المرحلة الثانوية، مجلة العلوم التربوية، المجلد 25، العدد الرابع، الجزء الأول، كلية الدراسات العليا للتربية، جامعة القاهرة، أكتوبر 2017م، ص 204.

[2] د. سحر فؤاد مجيد، الجرائم المستحدثة، مرجع سابق، ص 128.

يتضمن معلومات مهينة حول حياة الضحية الخاصة ونزاهتها، بقصد إيذائها[1]، مما يشكل تنمرًا إلكترونيًا عبر انتحال الهوية.

5- التنمر الإلكتروني باستخدام اسم مستعار:

يتضمن التظاهر بأنه شخص آخر محل ثقة عبر الإنترنت لإيذاء شخص أو مجموعة أشخاص. ويرتكب الجاني الجريمة بانتحال شخصية المجني عليه أو الضحية باستخدام اسم وهمي للإساءة إلى الآخرين، مما يظهر الضحية وكأنها هي من تنفذ السلوك الإجرامي.

وللحد من هذا النوع من التنمر، تتطلب مواقع التواصل الاجتماعي من المستخدمين استخدام هوياتهم الحقيقية ومعلوماتهم الشخصية الصحيحة وعدم إنشاء حسابات وهمية، التزامًا بمبدأ التعريف (Identity)[2]، حيث يمكن للمتنمر الإلكتروني أن يبقى مجهول الهوية باستخدام حسابات مؤقتة وأسماء مستعارة في غرف الدردشة، وبرامج التراسل الفوري، والهواتف الخلوية، والرسائل النصية، مما يسمح لهم بالتصرف بحرية ودون رادع من التقاليد أو المبادئ الاجتماعية.

6- التنمر الإلكتروني بواسطة الصور ومقاطع الفيديو:

تتمثل هذه الوسيلة في استيلاء المتنمر على صور ومقاطع فيديو شخصية تخص الضحية، قام الضحية بتداولها بين أصدقائه، فيقوم المتنمر بإعادة تداول هذه المواد كما هي أو بعد تعديلها وتغييرها، وربما تحويرها باستخدام برامج معالجة الصور والفيديو، مما يجعلها وسيلة لإنتاج مواد مخلة بالأخلاق أو الآداب العامة، والتي تشمل الصور، والكتابات، والأصوات. وفي حال توفر صور ومقاطع فيديو واضحة تتعلق بالإنتاج غير القانوني، ينتقل الفاعل بذلك إلى ارتكاب جريمة الاستغلال الجنسي عبر الإنترنت[3].

---

(1) High Court London, 24 July 2008, cité dans, Fabrice MATTATIA, Internet et les réseaux sociaux, que dit la loi ? Eyrolles, 2éme edition, 2016, p. 110.

(2) Richard STEPPE, The freedom of speech on social networking services, do we need protection against our own expression ?, www.law.kuleuven.be/jura/art/50n3/steppe.pdf, p. 563.

(3) د. سحر فؤاد مجيد، الجرائم المستحدثة، مرجع سابق، ص 134.

على سبيل المثال، يمكن إنشاء مجموعة على فيسبوك خاصة بطلاب المدرسة لمشاركة تجاربهم وذكرياتهم، ولكن يتم استغلالها من قبل بعض الطلاب لنشر صور المعلمين والتعليق عليها بتعليقات ساخرة وتوجيه السباب والألفاظ الخارجة علنًا، إضافة إلى ذم أنظمة المدرسة[1].

7- التنمر الإلكتروني عبر المحتوى الجنسي:

يتضمن إرسال محتوى جنسي أو نشر صور أو رسائل موحية جنسيًا عن شخص ما عبر الهواتف الخلوية، ومواقع التواصل الاجتماعي، والمنتديات الإلكترونية، أو غرف الدردشة. ويُعتبر الإفصاح أو نشر الصور الجنسية الخاصة دون إذن نوعًا من الانتقام الإباحي، ويشمل عادةً تحميل الصور الحميمة للضحية على الإنترنت من قبل شريك سابق لإحداث الإذلال أو الإحراج للضحية. ويؤدي هذا السلوك إلى تأثيرات نفسية سلبية على المجني عليهم، مما يدفعهم نحو الإحباط والاكتئاب.

8- التنمر الإلكتروني عبر المطاردة أو الملاحقة الإلكترونية:

يتضمن ملاحقة الأشخاص أو الشركات بشكل متكرر بهدف الإضرار بعملهم أو سمعتهم، فيقوم المتنمر بإرسال رسائل التحرش والتشويه للضحية لخلق حالة من التهديد، والخوف الشديد، والإذلال، أو الابتزاز للمجني عليه. وتعتبر المطاردة الإلكترونية شكلًا من أشكال المضايقة التي تشمل اتصالًا غير مرغوب فيه ومتكرر، أو تدخلًا في حياة شخص ما. وتستخدم هذه الوسيلة من قبل مروجي الشائعات بقصد التشهير عبر المدونات الإلكترونية، وغرف الدردشة، والمواقع الشخصية أو التجارية، ومواقع التواصل الاجتماعي[2].

---

[1] د. ياسر محمد اللمعي، المواجهة الجنائية لظاهرة التنمر الإلكتروني في ضوء السياسة التشريعية الحديثة، مرجع سابق، ص 19.

[2] المرجع السابق، ص 20.

الفرع الثاني

أسباب التنمر الإلكتروني وآثاره السلبية

أولًا- أسباب ودوافع التنمر الإلكتروني:

يتأثر التنمر الإلكتروني بعوامل متعددة تساهم في تشكيل سلوك الأفراد في التعامل مع الأجهزة الإلكترونية. وتتنوع هذه العوامل بين ما يتعلق بالبيئة المحيطة بالأفراد وسماتهم الشخصية، وما يرتبط بتوفر الأجهزة الإلكترونية وسهولة استخدامها، مما جعلها وسيلة مثالية لارتكاب أفعال التنمر. ويأتي ذلك في ظل غياب الرقابة الأخلاقية والاجتماعية على استخدام الإنترنت بمواقعه وتطبيقاته المختلفة. لكن، تظل البيئة المحيطة العامل الأساسي؛ نظرًا لتأثيرها القوي في تشكيل السمات الشخصية والنفسية والاجتماعية للأفراد من خلال قنوات التنشئة الاجتماعية. ويمكن تلخيص أهم هذه الأسباب في النقاط التالية:

1- العوامل الأسرية:

تشكل العوامل الأسرية مجموعة من الممارسات والسلوكيات التي تؤثر بشكل مباشر على خبرات الطفل والمراهق، بما في ذلك احتمالية تعرضهم للتنمر. فالأطفال والمراهقون الذين يعيشون في بيئات منزلية تتسم بالعنف والصراع وسوء المعاملة يكونون أكثر عرضة للتنمر. كذلك، فإن العيش مع والدين يعانيان من اضطرابات على أي مستوى قد يزيد من احتمالية تعرضهم للتنمر.

وتشير الدراسات إلى أن بعض العوامل الأسرية تلعب دورًا محوريًا في تشكل السلوك التنمري؛ فقد أظهرت الأبحاث أن العديد من الطلاب الذين يمارسون التنمر في مدارسهم هم في الواقع ضحايا في منازلهم، وينتمون إلى أسر تعاني من صعوبات في العلاقة بين الأب والأبناء، بالإضافة إلى تحديات اجتماعية ومالية، وغالبًا ما ينحدر هؤلاء التلاميذ من عائلات تفتقر إلى الدفء والحنان والنظام في المنزل، ويواجهون صعوبة في التعبير عن مشاعرهم ومشاركتها مع الآخرين. كما أن أولياء أمور الطلاب المتنمرين نادرًا ما يضبطون سلوكيات أبنائهم أو يراقبونهم، ويميلون إلى استخدام أساليب قاسية وعقابية في تربية أبنائهم[1].

---

[1] د. مشعل الأسمر البنتان، العوامل الاجتماعية المؤدية لسلوك التنمر لتلاميذ المرحلة المتوسطة بمنطقة حائل: دراسة من منظور الممارسة العامة في الخدمة الاجتماعية، مجلة كلية التربية الأساسية للعلوم التربوية والإنسانية، العدد (42)، جامعة بابل، العراق، فبراير 2019م، ص 105، منشور على الموقع الآتي:

وأظهرت الدراسات أيضًا أن للتنشئة الأسرية دورًا كبيرًا في ارتفاع معدلات العنف والتنمر بين الطلاب في المدارس؛ وتتجلى هذه الأسباب في أساليب التربية التي يعتمدها الأهل، مثل التذبذب في اتخاذ القرارات، وعدم الاتفاق على منهج موحد في الثواب والعقاب بين الوالدين، مما يؤدي إلى اختلاف في القوانين داخل المنزل، وينتج عنه طلاب يميلون إلى التمرد والتنمر على أقرانهم في المدارس. بالإضافة إلى ذلك، فإن التساهل في التربية وعدم معاقبة الأبناء على أخطائهم قد يؤدي إلى سلوكيات عنيفة منهم تجاه أقرانهم سواء في المدارس أم خارجها[1].

وقد تعود العوامل الأسرية المسؤولة عن ارتفاع نسبة التنمر إلى ميل الأسر في المجتمعات الحديثة إلى التركيز على تلبية الاحتياجات المادية للأبناء من مسكن وملبس ومأكل وتعليم وترفيه، على حساب الدور الأساسي في التربية والتقويم، وقد يكون هذا الإهمال نتيجة انشغال الأبوين عن تربية أبنائهم، وإلقاء المسؤولية على المدرسين أو المربيات، مما يؤدي إلى ضعف المتابعة التربوية.

وبذلك، فالعنف الأسري يمثل أحد أهم أسباب التنمر، فالطفل أو المراهق الذي ينشأ في بيئة أسرية يسودها العنف، سواء بين الزوجين أم تجاه الأبناء، يتأثر بما يشاهده أو بما يمارس عليه من عنف. ونتيجة لذلك، يميل الطفل أو المراهق الذي يتعرض للعنف في الأسرة إلى ممارسة العنف والتنمر تجاه أقرانه في المدرسة[2].

2- المناخ المدرسي:

لقد بلغ العنف في المؤسسات التعليمية المعاصرة مستويات غير مسبوقة، حيث وصلت حد الاعتداء اللفظي والجسدي على المعلمين من قبل الطلاب وأولياء أمورهم، مما أدى إلى تلاشي الحدود الفاصلة بين الاحترام الواجب بين الطالب ومعلمه، الأمر الذي أسفر عن تراجع هيبة المعلمين وتأثيرهم على الطلاب، وبالتالي شجع البعض على ممارسة التسلط والتنمر على

- **https://search.emarefa.net/ar/detail/BIM-893716.**

[1] أ. سعدية صالحي، مستوى التنمر المدرسي لدى التلاميذ: دراسة ميدانية على تلاميذ السنة الثالثة والرابعة متوسط بولايتي البيض وسعيدة، رسالة ماجستير، كلية العلوم الاجتماعية والإنسانية، قسم العلوم الاجتماعية، جامعة د. مولاي الطاهر سعيدة، الجزائر، 2017-2018م، ص 27، منشورة على الموقع الآتي:

- **https://bussh.univ-saida.dz/doc_num.php?explnum_id=1337.**

[2] د. ثناء هاشم محمد، واقع ظاهرة التنمر الإلكتروني لدى طلاب المرحلة الثانونية في محافظة الفيوم وسبل مواجهتها: دراسة ميدانية، مجلة جامعة الفيوم للعلوم التربوية والنفسية، العدد الثاني عشر، الجزء الثاني، 2019م، ص 208.

الآخرين. كما أن الاعتماد على أساليب التدريس التقليدية التي تركز على مركزية المدرس كمصدر وحيد للمعرفة وتمنحه السلطة المطلقة داخل الفصل، قد يدفعه إلى تبني العنف والإقصاء كوسيلة لحل المشكلات داخل الفصل، مما يساهم في توفير بيئة خصبة لنمو ظاهرة التنمر. بالإضافة إلى ذلك، فإن غياب الأنشطة الموازية داخل المدارس وحصر الحياة المدرسية في الأنشطة الرسمية التي تمارس داخل الفصل في إطار تنفيذ البرامج الدراسية يزيد من تفاقم هذه الظاهرة[1].

ويُعرَّف المناخ المدرسي بأنه مجموعة المعتقدات غير المكتوبة والقيم والاتجاهات والأطر الثقافية التي تحكم التفاعل بين الطلاب بعضهم البعض من جهة، وبينهم وبين المدرسة والمعلمين والإدارة من جهة أخرى[2]. ويمكن القول إن ضعف المناخ المدرسي، المتمثل في ضعف إحساس الطالب بالانتماء للمدرسة، وتدهور مستويات الاحترام المتبادل، وسوء المعاملة وغياب العدالة، يخلق بيئة مواتية للتنمر. بالإضافة إلى ذلك، فإن العلاقات المتوترة والتغيرات المفاجئة داخل المدرسة، والشعور بالإحباط والكبت، وقمع الطلاب، إلى جانب المناخ التربوي الذي يتسم بعدم وضوح الأنظمة المدرسية، وتردي مبنى المدرسة، واكتظاظ الصفوف، وأسلوب التدريس غير الفعال، كلها عوامل تؤدي إلى الإحباط، مما يدفع بعض الطلاب إلى سلوكيات سلبية، يظهر بعضها في شكل تنمر[3].

3- التأثير السلبي للأقران:

تلعب جماعة الأقران دورًا محوريًا في تعرض الفرد للتنمر، وذلك من خلال طبيعة العلاقات بينهم وسماتهم الفردية، فضلًا عن رفض الأقران وكراهيتهم. وقد أظهرت الدراسات أن الارتباط بجماعات الأقران التي تمارس سلوكيات لا اجتماعية يزيد من فرص العنف والسلوك العدواني. ويمكن للأقران في المجتمع الافتراضي أن يكونوا متفرجين على التنمر الإلكتروني، مما يشبه ما

---

[1] د. ثناء هاشم محمد، واقع ظاهرة التنمر الإلكتروني لدى طلاب المرحلة الثانونية في محافظة الفيوم وسبل مواجهتها، مرجع سابق، ص 206.

[2] Sara Pabian, Heidi Vandebosch, Short-term longitudinal relationships between adolescents (cyber)bullying I perpetration and bonding to school and teachers, International Journal of Behavioral Development, 2016, Vol. 40 (2), p. 16.

[3] أ. فاطمة زهراء صوفي، المناخ المدرسي وعلاقته بالتنمر المدرسي لدى تلاميذ المرحلة الثانوية: دراسة ميدانية على عينة من تلاميذ الثانوي بسعيدة، رسالة ماجستير، كلية العلوم الاجتماعية والإنسانية، قسم العلوم الاجتماعية، جامعة د. مولاي الطاهر سعيدة، الجزائر، 2017-2018م، ص 29، منشورة على الموقع الآتي:

- **https://bussh.univ-saida.dz/doc_num.php?explnum_id=1525.**

يحدث في المجتمع الواقعي بعيدًا عن الإنترنت، وتؤدي هذه التفاعلات السلبية بين الأقران إلى زيادة مستويات التنمر الإلكتروني من خلال تعزيز ثقافة جماعية تكافئ السلوك المتنمر[1].

وبذلك، نجد أن جماعة الأقران تلعب أدوارًا متعددة في إثارة السلوك التنمري أو تعزيزه، فقد تقوي الجماعة بعض الأفراد على غيرهم تحت ضغط الأقران، وذلك لكسب الشعبية، وهذا يظهر بوضوح في مرحلة المراهقة، حيث يعتمد المراهق في تقديره لذاته وإظهار قدراته على جماعة الأقران، التي تلعب دورًا كبيرًا في نموه الاجتماعي[2].

4- الإعلام والثورة التقنية:

تتعدد الأسباب الإعلامية والتقنية التي تسهم في انتشار ظاهرة التنمر الإلكتروني، ومن أبرزها:

أ- **الألعاب الإلكترونية:** تعتمد العديد من الألعاب الإلكترونية على مفاهيم مثل القوة الخارقة، وسحق الخصوم، واستخدام كافة الوسائل لتحقيق أعلى النقاط والانتصار، دون أن تحمل أي أهداف تربوية. وهذا يجعل المراهقين المدمنين على هذا النوع من الألعاب ينظرون إلى الحياة اليومية، بما في ذلك الحياة المدرسية، على أنها امتداد لهذه الألعاب، مما يدفعهم إلى ممارسة حياتهم في مدارسهم وبين معارفهم والمحيطين بهم بنفس الطريقة العدائية التي يتبنونها في الألعاب[3].

ب- **انتشار أفلام العنف:** إلى جانب الألعاب الإلكترونية، يشهد التلفاز تزايدًا ملحوظًا في عرض أفلام العنف، سواء تلك الموجهة للكبار أم الصغار، وتتضمن هذه الأفلام مشاهد متكررة من القتل الهمجي والاستهانة بالنفس البشرية، مما يشكل خطرًا كبيرًا، خاصةً عند الأطفال والمراهقين الذين يميلون إلى تصديق ما يشاهدونه وتقليده. ويزيد هذا الميل إلى

---

[1] Sheryl A. Hemphill, PhD, and others, Predictors of Traditional and Cyber-Bullying Victimization: A Longitudinal Study of Australian Secondary School Students, Journal of Interpersonal Violence, Vol. 30 (15), 2015, p. 2570.

[2] أ. فاطمة زهراء صوفي، المناخ المدرسي وعلاقته بالتنمر المدرسي لدى تلاميذ المرحلة الثانوية، مرجع سابق، ص 29.

[3] أ. معاوية محمود أبو غزال، الاستقواء وعلاقته بالشعور والوحدة والدعم الاجتماعي، المجلة الأردنية في العلوم التربوية، المجلد الخامس، العدد الثاني، كلية التربية، جامعة اليرموك، إربد، الأردن، 2009م، ص 89 وما بعدها، منشور على الموقع الآتي:

- **https://journals.yu.edu.jo/jjes/Issues/2009/Vol5No2/art1.pdf.**

التقليد وإعادة إنتاج ما يعرض في هذه الأفلام من احتمالية تبني سلوكيات عنيفة في الواقع، مما يسهم في انتشار ظاهرة التنمر الإلكتروني[1].

5- الأسباب المجتمعية:

قد تُعزى الأسباب المجتمعية المسؤولة عن انتشار التنمر في المجتمع إلى عدة عوامل، منها: غياب الوعي بخطورة العنف داخل المدارس بكافة أشكاله، وضعف المشاركة المجتمعية في التصدي لهذه الظاهرة. بالإضافة إلى ذلك، يعاني المجتمع من عدم القدرة على الحد من التسرب المدرسي، وتراجع دور الأسرة في توعية الأطفال وتوجيههم، وفي تعديل سلوكياتهم العنيفة، كما يسهم غياب الوعي بأساليب التنشئة السليمة، وضعف ثقافة حقوق الإنسان، وسوء الأحوال الاقتصادية والاجتماعية للأسر، في دفع الأطفال والمراهقين نحو العنف. هذا، إلى جانب الترويج الإعلامي لثقافة العنف في بعض البرامج، والأفلام، وألعاب الكمبيوتر[2].

6- الأنانية والشعور بالقوة من خلال الغموض:

يعد الشعور بالغموض وعدم الكشف عن الهوية أحد الأسباب الرئيسية التي تجعل التنمر الإلكتروني شائعًا؛ حيث يمكن للمتنمرين الإلكترونيين الهجوم على الآخرين دون الخوف من التعرض للعواقب، مما يشجعهم على القيام بأفعال عدوانية. ووفقًا لدراسة أجرتها Pew Research Center في عام 2022، فإن 53% من المراهقين الذين يستخدمون الإنترنت بشكل مستمر تعرضوا للتنمر الإلكتروني مقارنة بـ 40% ممن يستخدمون الإنترنت بشكل أقل[3].

7- التأثيرات الثقافية والمجتمعية:

بعض الثقافات قد تتسامح مع السلوكيات العدوانية أو تشجعها، مما يجعل التنمر الإلكتروني سلوكًا مقبولًا أو غير معاقب عليه. فالمجتمعات التي لا تولي اهتمامًا كافيًا بمكافحة التنمر قد تشهد انتشارًا أكبر لهذه الظاهرة. على سبيل المثال، أشارت دراسة في الولايات المتحدة إلى أن

---

(1) Bulach, C. Impiementing a character education cuiriculum and assessing its impact on ctud ent behavior. The clearing 2002, p. 11.

(2) د. ثناء هاشم محمد، واقع ظاهرة التنمر الإلكتروني لدى طلاب المرحلة الثانوية في محافظة الفيوم وسبل مواجهتها، مرجع سابق، ص 210.

(3) Emily A. Vogels, Teens and Cyberbullying 2022:

- **https://www.pewresearch.org/internet/2022/12/15/teens-and-cyberbullying-2022/.**

70% من المراهقين السود يرون أن التنمر الإلكتروني يشكل مشكلة كبيرة مقارنة بـ 46% فقط من المراهقين البيض[1].

8- الاضطرابات النفسية:

بعض الأفراد قد يعانون من اضطرابات نفسية مثل اضطراب الشخصية المعادية للمجتمع أو اضطرابات السيطرة على الدوافع، مما يزيد من احتمالية تورطهم في التنمر الإلكتروني. فقد تستخدم هذه الفئة التنمر كوسيلة للتعبير عن مشاكلهم الداخلية أو كوسيلة للتعامل مع ضغوطهم النفسية.

9- الجهل بالعواقب القانونية:

قد يجهل البعض العواقب القانونية للتنمر الإلكتروني، مما يشجعهم على المشاركة فيه دون إدراك بالمخاطر القانونية المحتملة، فيمكن أن يزيد هذا النقص في الوعي من شيوع التنمر الإلكتروني، خاصة في البيئات التي لا تُفرض فيها عقوبات رادعة بفعالية.

ثانيًا- الآثار السلبية للتنمر الإلكتروني:

للتنمر الإلكتروني آثار سلبية واسعة النطاق تتجاوز حدود الفرد لتشمل المجتمع بأسره، حيث تؤثر هذه الظاهرة بشكل مباشر على الضحايا والمتنمرين، وتتعدى ذلك لتشكل تهديدًا على النسيج الاجتماعي والاستقرار العام. ويمكن تلخيص بعض هذه الآثار على النحو التالي:

1- الآثار السلبية للتنمر الإلكتروني على الضحايا:

يترتب على التنمر آثار مؤلمة ومهينة تلحق بالضحايا، حيث يؤدي إلى شعورهم بالبؤس والضيق والارتباك، مما يفقدهم احترامهم لذواتهم ويشعرهم بالقلق وفقدان الأمان. بالإضافة إلى ذلك، قد يتعرض الضحايا لإصابات بدنية ويعانون من تدهور في تركيزهم وانتباههم في العملية التعليمية. وفي حالات كثيرة، يتجنبون الذهاب إلى المدرسة هربًا من التنمر، مما يعمق إحساسهم بالخوف وانعدام الأمان، ويواجهون صعوبة في تكوين صداقات مع أقرانهم ويعانون من ضعف في تطوير المهارات الاستقلالية، مما يجعلهم أكثر عرضة للاستغلال ونقص في مهارات تأكيد الذات، وتظهر لديهم أعراض جسدية ونفسية مثل الصداع وآلام البطن.

---

[1] Emily A. Vogels, Teens and Cyberbullying 2022:

- **https://www.pewresearch.org/internet/2022/12/15/teens-and-cyberbullying-2022/.**

وفي بعض الحالات، قد يصل الأمر بالضحايا إلى مستوى من تدني الذات يجعلهم يرون الانتحار كخيار وحيد للخلاص من معاناتهم. وعلى المدى البعيد، فإن التنمر المستمر خلال سنوات الدراسة يمكن أن يترك آثارًا سلبية طويلة الأمد تمتد إلى مرحلة ما بعد المدرسة، حيث يظهر الضحايا في السنوات الأولى من حياتهم ميولًا أكبر للاكتئاب وانخفاض في تقدير الذات مقارنة بأقرانهم الذين لم يتعرضوا للتنمر[1].

وبذلك يمكن تلخيص الآثار الناجمة عن التنمر على الضحايا على النحو التالي:

- تتحول الضحية إلى شخص مرفوض وغير مرغوب فيه، مما يعزز شعورها بالعزلة.
- يؤدي التنمر إلى إحداث أضرار نفسية وعاطفية وسلوكية طويلة الأمد، بما في ذلك الاكتئاب، والشعور بالوحدة، والانعزال، والقلق، والإدمان، وإيذاء النفس، بالإضافة إلى تدهور العلاقات الاجتماعية وفقدان الثقة بالآخرين.
- قد تلجأ الضحية إلى سلوكيات عدوانية كرد فعل على التنمر، وقد تتحول بمرور الوقت إلى متنمر أو تصبح شخصًا عنيفًا.
- يتزايد انسحاب الضحية من الأنشطة الاجتماعية سواء في الأسرة أم المدرسة، حتى يصبح شخصًا صامتًا ومنعزلًا تمامًا.
- يشكل التنمر سببًا رئيسيًا في حالات الانتحار المتزايدة بين الضحايا.
- يعاني ضحايا التنمر من اضطرابات في النوم، وصداع، وآلام في المعدة، وحالات من الخوف والذعر.
- يتدنى تحصيلهم الدراسي نتيجة للغياب المستمر أو الانقطاع عن الدراسة خوفًا من مواجهة المتنمرين.

2- الآثار السلبية للتنمر الإلكتروني على المتنمرين:

التنمر ليس فقط سلوكًا انعزاليًا يمارسه المتنمرون، بل هو أيضًا جزء من نمط سلوكي يتعارض مع المبادئ المجتمعية ويقوضها، مما يؤدي إلى إضعاف القواعد التي تنظم المجتمع.

---

[1] يراجع: د. أحمد فكري بهنساوي، د. رمضان علي حسن، التنمر المدرسي وعلاقته بدافعية الإنجاز لدى تلاميذ المرحلة الإعدادية، مجلة كلية التربية، العدد (17)، جامعة بورسعيد، يناير 2015م، ص 17؛ د. سليمة سايحي، د. أسماء سايحي، البرامج العالمية لمكافحة التنمر المدرسي: برنامج دان ألويس نموذجًا، المجلة الدولية للدراسات التربوية والنفسية، العدد 4، المركز الديمقراطي العربي ببرلين، ألمانيا، مارس 2019م، ص 103-104، منشور على الموقع الآتي: https://democraticac.de/wp-content/uploads/2019/03/؛ د. ثناء هاشم محمد، واقع ظاهرة التنمر الإلكتروني لدى طلاب المرحلة الثانوية في محافظة الفيوم وسبل مواجهتها، مرجع سابق، ص 204-205.

فالأفراد الذين اعتادوا ممارسة التنمر، وخاصة الذكور، يكونون أكثر عرضة للانخراط في سلوكيات اجتماعية غير مقبولة، مثل الاعتداء على ممتلكات الآخرين، والسرقة من المحلات، والتغيب عن المدرسة، واستخدام المخدرات بصفة متكررة[1].

ويمكن تلخيص الآثار السلبية على المتنمرين في النقاط التالية:

- الحرمان والطرد من المدرسة، مما يؤدي إلى حرمانهم من الاستفادة من البرامج التعليمية المتاحة لهم.
- إدمان الكحول والمخدرات، والتورط في أنشطة إجرامية ومخالفات قانونية.
- الانخراط في العراك المستمر، وتخريب الممتلكات، والانقطاع عن الدراسة.
- ممارسة النشاطات الجنسية المبكرة والانحراف الجنسي.

3- الآثار السلبية للتنمر الإلكتروني على المجتمع:

التنمر الإلكتروني لا يؤثر فقط على الأفراد المتضررين، بل يمتد تأثيره السلبي إلى المجتمع والدولة ككل، ويمكن تلخيص الآثار السلبية للتنمر الإلكتروني على المجتمع على النحو التالي:

- **تقويض القيم الاجتماعية والمبادئ الأخلاقية:** يسهم التنمر الإلكتروني في تدهور القيم الاجتماعية، حيث يعزز السلوكيات العدوانية ويقلل من روح التسامح والتفاهم بين الأفراد، ويؤدي هذا إلى تفكك النسيج الاجتماعي، ويؤدي إلى خلق بيئة يسودها الخوف والعداء بدلًا من التعاون والاحترام المتبادل.
- **زيادة معدلات الجريمة والعنف:** يساهم التنمر الإلكتروني في زيادة معدلات الجريمة، خاصة بين الشباب الذين قد يتحولون إلى سلوكيات عدوانية نتيجة التأثر بالعنف الإلكتروني. ويمكن أن يؤدي هذا إلى ارتفاع معدلات الجرائم الإلكترونية، والاعتداءات الجسدية، وغيرها من الأنشطة غير القانونية التي تضع ضغطًا إضافيًا على الأجهزة الأمنية والقضائية في الدولة.
- **تدهور الصحة النفسية العامة:** انتشار التنمر الإلكتروني يؤثر على الصحة النفسية لأفراد المجتمع بشكل عام، مما يؤدي إلى زيادة في معدلات الاكتئاب، والقلق، ومحاولات الانتحار. ويضع هذا عبئًا إضافيًا على الأنظمة الصحية، ويؤدي إلى زيادة

---

[1] يراجع: د. أحمد فكري بهنساوي، د. رمضان علي حسن، التنمر المدرسي وعلاقته بدافعية الإنجاز لدى تلاميذ المرحلة الإعدادية، مرجع سابق، ص 17؛ د. سليمة سايحي، د. أسماء سايحي، البرامج العالمية لمكافحة التنمر المدرسي، مرجع سابق، ص 103-104؛ د. ثناء هاشم محمد، واقع ظاهرة التنمر الإلكتروني لدى طلاب المرحلة الثانونية في محافظة الفيوم وسبل مواجهتها، مرجع سابق، ص 203-204.

التكاليف المتعلقة بالعلاج النفسي والرعاية الصحية، مما يؤثر سلبًا على الاقتصاد الوطني.

- **التأثير السلبي على الاقتصاد:** يمكن أن يؤدي التنمر الإلكتروني إلى تراجع الإنتاجية في أماكن العمل بسبب تدهور الحالة النفسية للعاملين، وزيادة معدلات التغيب عن العمل. كما يمكن أن يؤثر على سمعة الشركات والمؤسسات، خاصة إذا استُخدمت منصات التواصل الاجتماعي كوسيلة للتشهير أو نشر معلومات مضللة، مما يؤثر سلبًا على الاستثمارات والأعمال التجارية.
- **إضعاف الثقة في المؤسسات الرقمية:** يؤدي انتشار التنمر الإلكتروني إلى تقويض الثقة في المنصات الرقمية والمؤسسات التي تستخدمها، مما يدفع الأفراد إلى الانسحاب من المشاركة في المجتمع الرقمي. ويؤثر هذا سلبًا على الاقتصاد الرقمي للدولة ويضعف من قدرة المجتمع على الاستفادة من التكنولوجيا لأغراض التنمية والتطوير.
- **زيادة الأعباء على النظام القانوني:** يؤدي انتشار التنمر الإلكتروني إلى زيادة القضايا القانونية المتعلقة بالجرائم الإلكترونية، مما يضع ضغطًا على النظام القانوني والقضائي، ويتطلب هذا موارد إضافية للتعامل مع القضايا، ويؤدي إلى تأخير في تحقيق العدالة.

في ضوء هذه الآثار السلبية، يصبح من الضروري أن تتبنى الدولة سياسات وإجراءات قوية لمكافحة التنمر الإلكتروني، من خلال تعزيز التشريعات، وتطوير برامج توعية فعالة، وتوفير الدعم النفسي والاجتماعي للضحايا، لحماية المجتمع والدولة من تبعات هذه الظاهرة.

المبحث الثاني

سلطات الضبط الإداري الإلكتروني في مواجهة التنمر الإلكتروني

تمهيد وتقسيم:

تتفق معظم الدساتير العالمية على ضرورة كفالة حريات الأفراد، ولكن إذا تُرك الأفراد دون توجيه أو تنظيم عند ممارستهم لهذه الحريات، فقد يتحول المجتمع إلى فوضى وتسلط، مما يؤدي إلى تهديد سلامة الأفراد وأمنهم. ومن هنا، يظهر التحدي في إيجاد توازن دقيق بين حق الفرد في ممارسة حرياته وحق المجتمع في المحافظة على أمنه وسلامته. ولهذه الغاية، ظهرت أهمية الضبط الإداري الإلكتروني كأحد أهم أدوات الدولة في تنظيم الحريات الفردية وتحقيق المصلحة العامة.

ومع ظهور أنماط جديدة من الجرائم الإلكترونية، والتي لم تكن مألوفة في السابق، وخصوصًا مع بداية عصر الانفجار المعلوماتي، يصبح من الضروري توقع ظهور المزيد من هذه الأنماط الجديدة، مما يتطلب تحديث الأنظمة والتشريعات والأجهزة الأمنية المتخصصة لمعالجة تلك الجرائم، ويستدعي هذا الأمر تطوير أساليب التحقيق والتفتيش فيها.

فالتحقيق في الجرائم الإلكترونية، بما في ذلك التنمر الإلكتروني، يتطلب من المحققين مهارات خاصة تشمل الذكاء والفطنة وقوة الملاحظة وسرعة البديهة، بالإضافة إلى جهود مكثفة في البحث عن الأدلة، والتي غالبًا ما تكون غير مادية وتختلف عن تلك التي تعتمد عليها الجرائم التقليدية. فإن غياب الآثار المادية التقليدية مثل بصمات الأصابع أو بقع الدم يجعل من الصعب إثبات الجرائم الإلكترونية، مما يستوجب البحث عن أدلة بديلة.

ولا شك أن الحصول على هذه الأدلة يتطلب وجود منظومة قانونية وقضائية متخصصة وفعالة في مجال المعلومات والتكنولوجيا، تتولى مهمة التحقيق والتفتيش في هذا النوع من الجرائم.

كما تُعد المواجهة التشريعية أحد أهم وسائل وإجراءات أجهزة الضبط الإداري الإلكتروني في التصدي للتنمر الإلكتروني؛ حيث إن وضع تشريعات دقيقة ومحددة تهدف إلى تنظيم سلوك الأفراد في الفضاء الإلكتروني، يُسهم بشكل فعال في حماية المجتمع من الأضرار التي قد تنجم عن ممارسات التنمر الإلكتروني. ولا تقتصر هذه التشريعات على تعريف الأفعال المجرمة فحسب، بل تمتد أيضًا لتحديد العقوبات المناسبة وتوفير آليات تنفيذ فعالة لضمان الردع

والتطبيق العادل للقانون. إضافة إلى ذلك، تُعزز المواجهة التشريعية من قدرة السلطات المختصة على متابعة ورصد الأنشطة الإلكترونية المشبوهة، مما يتيح التعامل مع الجرائم الإلكترونية بفعالية وسرعة، وتحقيق العدالة في مواجهة هذه الجرائم الحديثة. ومن هنا، تظهر الحاجة الملحة لوجود وسائل وإجراءات قوية للضبط الإداري الإلكتروني لمواجهة ظاهرة التنمر الإلكتروني وضمان حماية الأفراد والمجتمع من آثاره السلبية.

وهديًا على ما تقدم، يقسم هذا المبحث إلى ثلاثة مطالب على النحو الآتي:

- **المطلب الأول:** الإطار التشريعي لمواجهة التنمر الإلكتروني.
- **المطلب الثاني:** وسائل الضبط الإداري الإلكتروني في مواجهة التنمر الإلكتروني.
- **المطلب الثالث:** إجراءات الضبط الإداري الإلكتروني في مواجهة التنمر الإلكتروني.

المطلب الأول

الإطار التشريعي لمواجهة التنمر الإلكتروني

تُعتبر جريمة التنمر الإلكتروني نموذجًا للجريمة المستحدثة التي تستغل التطورات الثقافية الحديثة كوسيلة لارتكابها. وفي هذا السياق، يمكن التركيز على النصوص القانونية القابلة للتطبيق على حالات التنمر الإلكتروني من الناحية القانونية، حيث سعت التشريعات الفرنسية والمصرية إلى حماية الحقوق والحريات، ومنعت جميع أشكال الاعتداء عليها، مع فرض عقوبات جنائية على مرتكبيها. وبالنظر إلى تعريف جريمة التنمر، يتضح أن المتنمر الإلكتروني يتعمد التدخل في خصوصيات الضحية وانتهاك حرمة حياتها الخاصة. وسوف نستعرض موقف المشرع الفرنسي والمصري من التنمر الإلكتروني، ثم نتناول موقفيهما من بعض صوره وأشكاله، وذلك على النحو الآتي:

أولًا- العقوبات المقررة لجريمة التنمر الإلكتروني:

عاقب المشرع الفرنسي على التحرش المعنوي وفقًا لنصوص القانون بطريقتين:

1. **الطريقة الأولى:** في حالة ما إذا وقع السلوك الإجرامي داخل بيئة العمل، فقد نصت المادة رقم (222-33-2) من قانون العقوبات الفرنسي على عقوبة الحبس لمدة قد تصل إلى عامين، وبغرامة تصل إلى ثلاثين ألف يورو. ولتطبيق هذه العقوبة، يشترط توافر العنصر المفترض لهذه الجريمة، وهو وجود علاقة عمل بين الجاني والمجني عليه، أي بين المتنمر والمتنمر عليه، وتُرتكب الجريمة في إطار هذه العلاقة. وفي حال

انتفاء علاقة العمل، لا تُطبق الجريمة المنصوص عليها في هذه المادة. كما يشترط أن يكون السلوك الجنائي المرتكب ضمن حدود علاقة العمل؛ على سبيل المثال، إذا أشار المتهم بصفته رئيسًا إداريًا أثناء اجتماع عام مع الموظفين إلى عدم كفاءة المجني عليه في أداء العمل، فإن ذلك لا يُعد من قبيل التنمر الذي يحدث في بيئة العمل[1].

2. **الطريقة الثانية:** تتعلق بالعقوبة التي تقع على الزوج أو الشريك المرتبط باتفاق تضامن مدني، أو الخليل، وذلك في إطار العلاقة الزوجية، أو اتفاق التضامن المدني، أو على الشريك خارج علاقة الزوجية أو اتفاق التضامن المدني (الخليل أو العشيق). فقد نصت الفقرة الأولى من المادة رقم (222-33-2-1) من قانون العقوبات الفرنسي على أنه: "إن التحرش بالزوج أو الشريك المرتبط بعقد تضامن مدني أو العشير، من خلال أقوال أو سلوكيات متكررة تهدف أو تؤدي إلى تدهور في ظروف حياته/حياتها مما يترتب عليه تدهور في صحته/صحتها الجسدية أو العقلية، يعاقب عليه بالسجن لمدة ثلاث سنوات وغرامة قدرها 45,000 يورو إذا كانت هذه الأفعال قد تسببت في عجز كلي عن العمل لمدة ثمانية أيام أو أقل أو لم تؤدِ إلى أي عجز عن العمل. وتصل العقوبة إلى السجن لمدة خمس سنوات وغرامة قدرها 75,000 يورو إذا تسببت هذه الأفعال في عجز كلي عن العمل لمدة تزيد عن ثمانية أيام أو ارتكبت في حضور قاصر وشهدها.

وتُطبق نفس العقوبات عندما تُرتكب هذه الجريمة من قِبل زوج سابق أو عشير سابق للضحية، أو شريك سابق مرتبط بها بعقد تضامن مدني.

وتصل العقوبات إلى السجن لمدة عشر سنوات وغرامة قدرها 150,000 يورو إذا أدى التحرش إلى انتحار الضحية أو محاولة الانتحار[2]".

---

[1] د. حسين بن سعيد الغافري، جريمة التنمر الإلكتروني عبر وسائل التواصل الاجتماعي، مرجع سابق، ص 1141.

[2] Article 222-33-2-1Version en vigueur depuis le 01 août 2020:
"Le fait de harceler son conjoint, son partenaire lié par un pacte civil de solidarité ou son concubin par des propos ou comportements répétés ayant pour objet ou pour effet une dégradation de ses conditions de vie se traduisant par une altération de sa santé physique ou mentale est puni de trois ans d'emprisonnement et de 45 000 € d'amende lorsque ces faits ont causé une incapacité totale de travail inférieure ou égale à huit jours ou n'ont entraîné aucune incapacité de travail et de cinq ans d'emprisonnement et de 75 000 € d'amende lorsqu'ils ont causé une incapacité

ونستخلص مما تقدم تأكيد المشرع الفرنسي على مبدأ تجريم كافة أشكال التحرش المعنوي والجسدي، مستندًا إلى فكرة حماية الصحة البدنية والنفسية كحق أساسي لا يجوز المساس به. كما يبرز المشرع مبدأ التناسب في العقوبة، حيث تتفاوت العقوبات وفقًا لجسامة الضرر الناجم عن الفعل المُجرّم، مع مراعاة الظروف المشددة مثل وجود قاصر أو ارتباط الجاني بالضحية بعلاقة سابقة. ويتجلى كذلك مبدأ المسؤولية الجنائية المشددة في حال أدت الأفعال إلى نتائج خطيرة كتسببها في انتحار الضحية أو محاولتها، مما يعكس حرص المشرّع على التصدي لنتائج الأفعال الإجرامية بأقصى درجات الحزم.

أما بالنسبة لعقوبة التنمر في التشريع المصري، فقد نص المشرع المصري على عقوبة جريمة التنمر وفقًا للمادة رقم (309 مكررًا ب) من قانون العقوبات، حيث نصت الفقرة الثانية على أنه: "مع عدم الإخلال بأي عقوبة أشد منصوص عليها في أي قانون آخر، يُعاقب المتنمر بالحبس لمدة لا تقل عن ستة أشهر وبغرامة لا تقل عن عشرة آلاف جنيه ولا تزيد على ثلاثين ألف جنيه، أو بإحدى هاتين العقوبتين".

فمن خلال النص السابق، يتضح أن المشرع المصري قد قرر عقوبتين لمرتكب جريمة التنمر:

1. **العقوبة الأولى سالبة للحرية:** وهي عقوبة الحبس، حيث رفع المشرع الحد الأدنى لهذه العقوبة عن حدها الأدنى العام، ليصبح لا يقل عن ستة أشهر. أما الحد الأقصى فهو الحد العام المقرر لعقوبة الحبس دون تغيير وهو ثلاث سنوات. ويعكس هذا النص حرص المشرع على مواجهة جريمة التنمر بعقوبات رادعة؛ نظرًا لانتشار هذه الظاهرة بشكل متزايد داخل المجتمع المصري في الآونة الأخيرة وعلى كافة المستويات، لا سيما من خلال أدوات التواصل الاجتماعي المتعددة.
2. **العقوبة الثانية هي الغرامة:** فقد حدد المشرع لهذه العقوبة حدًا أدنى لا يقل عن عشرة آلاف جنيه، وحدًا أقصى لا يزيد على ثلاثين ألف جنيه. ولم يلزم المشرع الجمع بين

---

totale de travail supérieure à huit jours ou ont été commis alors qu'un mineur était présent et y a assisté.

Les mêmes peines sont encourues lorsque cette infraction est commise par un ancien conjoint ou un ancien concubin de la victime, ou un ancien partenaire lié à cette dernière par un pacte civil de solidarité.

Les peines sont portées à dix ans d'emprisonnement et à 150 000 € d'amende lorsque le harcèlement a conduit la victime à se suicider ou à tenter de se suicide".

عقوبتي الحبس والغرامة، بل ترك الأمر لتقدير المحكمة المختصة، حيث يجوز لها أن تجمع بين العقوبتين، أو أن تكتفي بواحدة منهما، أو أن تأمر بإيقاف تنفيذ العقوبة، سواء عند الجمع بين العقوبتين أم عند الحكم بإحداهما فقط. وتُطبق العقوبات المنصوص عليها في الفقرة الثانية من المادة رقم (309 مكررًا ب) في حال عدم وجود عقوبة أشد منصوص عليها في قانون آخر، فإذا كان سلوك المتهم ينطوي على أوصاف متعددة، من بينها التنمر، فلا تُطبق عقوبة التنمر إلا إذا كانت هي الأشد.

ومن ثم، فإن المشرع المصري قد أقر العقاب على جريمة التنمر من خلال عقوبة الحبس أو الغرامة، حيث قرر الحبس لمدة لا تقل عن ستة أشهر، وغرامة لا تقل عن عشرة آلاف جنيه، ولا تزيد على ثلاثين ألف جنيه، أو بإحدى هاتين العقوبتين. كما شدد العقوبة في حال توافر ظرفين مشددين؛ أولهما: إذا ارتكبت الجريمة من قبل شخصين أو أكثر، وثانيهما: إذا كان الفاعل من أصول المجني عليه أو من المتولين تربيته أو رعايته أو ممن لهم سلطة عليه. كذلك، شدد المشرع العقوبة إذا كان المجني عليه تحت وصاية الجاني بمقتضى القانون أو حكم قضائي، أو كان خادمًا لدى الجاني. وفي هذه الحالات، تكون العقوبة الحبس لمدة لا تقل عن سنة، وغرامة لا تقل عن عشرين ألف جنيه، ولا تزيد على مائة ألف جنيه، أو بإحدى هاتين العقوبتين، مع مضاعفة الحد الأدنى للعقوبة عند اجتماع الظرفين المشددين. وفي حالة العود، تضاعف العقوبة في حديها الأدنى والأقصى.

ويتضح من ذلك أن المشرع المصري قد ميز في العقاب على جريمة التنمر بين حالتيها العادية والمشددة، وهو ما يتيح للقاضي إمكانية تحقيق العدالة من خلال تفريد العقاب وفقًا للظروف المحيطة بكل قضية[1].

وهديًا على ما تقدم، يُعتبر التشريع المصري أفضل من نظيره الفرنسي في مواجهة جريمة التنمر؛ نظرًا لشمولية نصوصه التي توفر تغطية قانونية أوسع لا تقتصر على بيئات معينة، بل تمتد لتشمل جميع الحالات التي قد يقع فيها التنمر، مما يعزز قدرة القانون على حماية كافة الفئات المتضررة. كما يتميز التشريع المصري بالمرونة في تحديد العقوبة؛ حيث منح المشرع للقاضي سلطة تقديرية واسعة لاختيار العقوبة المناسبة بين الحبس والغرامة أو الجمع بينهما، بما يتيح تكييف العقوبة وفقًا لخطورة الجريمة وظروف المتهم الشخصية. إضافة إلى ذلك، يميز التشريع المصري بين الحالات العادية والمشددة للتنمر، مع تشديد العقوبة في الحالات التي

---

[1] د. حسين بن سعيد الغافري، جريمة التنمر الإلكتروني عبر وسائل التواصل الاجتماعي، مرجع سابق، ص 1144-1145.

تتطلب ذلك، مما يعكس وعي المشرع بخطورة بعض أشكال التنمر وضرورة مواجهتها بعقوبات أكثر صرامة. وأخيرًا، يضمن التشريع المصري تكامله مع التشريعات الأخرى، حيث ينص على عدم تعارضه مع عقوبات أشد واردة في قوانين أخرى، مما يعزز من انسجام وتكامل النظام القانوني.

ثانيًا- التحرش الإلكتروني:

يُقصد بالتحرش الإلكتروني بأنه: سلوك عدواني متعمد يرتكبه فرد أو مجموعة أفراد باستخدام الوسائل الإلكترونية للتواصل، وذلك من خلال تكرار مضايقة الضحية بوضعها في موقف ضعيف أو تجعلها غير قادرة على الدفاع عن نفسها بسهولة[1]. ويتمثل هذا السلوك الإجرامي في عدة صور، منها نشر صور أو مقاطع فيديو للضحية في أوضاع غير لائقة، أو توجيه الإهانات أو التعليقات ذات الطابع الجنسي عبر الإنترنت أو من خلال الهواتف المحمولة. ويُعتبر التحرش الجنسي الإلكتروني أحد أشكال التحرش الإلكتروني التي تنتشر بشكل كبير على مواقع التواصل الاجتماعي، وفي المنتديات وغرف الدردشة الإلكترونية.

وفيما يتعلق بموقف المشرع الفرنسي من التحرش الإلكتروني؛ فقد نص قانون العقوبات، في المادة 222-33 المعدلة بالقانون رقم 703 لسنة 2018، على تجريم التحرش الجنسي، فوفقًا لهذه المادة، يُعد التحرش الجنسي جريمة إذا تم فرضه على شخص عن طريق القول أو الإشارة أو أي وسيلة أخرى، بشرط أن تكون لهذه الكلمات أو التصرفات دلالة جنسية أو تؤدي إلى تقويض كرامة الشخص أو تثير فيه الخوف أو الإهانة. ويُعاقب على هذه الجريمة بالسجن لمدة تصل إلى سنتين وغرامة مالية لا تتجاوز 30,000 يورو.

وتُشدد العقوبة لتصل إلى السجن لمدة ثلاث سنوات وغرامة مالية لا تزيد عن 45,000 يورو في الحالات التالية:

- **الحالة الأولى:** إذا تم التحرش الجنسي عبر الوسائل الإلكترونية، مثل الاتصال عبر الإنترنت أو أي وسيلة رقمية أو إلكترونية أخرى.
- **الحالة الثانية:** إذا كانت الضحية قاصرًا، حيث تُطبق نفس العقوبة المشددة إذا وقعت الجريمة على قاصر لم يتجاوز سن الخامسة عشرة وقت ارتكاب الجريمة.

---

[1] N. TIPPETT, Cyberbullying: Its nature and impact in secondary school pupils. Journal of Child, Psychology and Psychiatry, 2008, N° 49,p 376.

- **الحالة الثالثة:** إذا استُغل ضعف خاص في الضحية، سواء بسبب السن أو المرض أو العجز، سواء كان العجز بدنيًا أو عقليًا، أو في حالة الحمل.
- **الحالـة الرابعـة:** إذا كـان التحـرش الجنسـي موجّهًـا لشـخص يعـاني مـن ضـعف أو عـدم استقرار في وضعه الاقتصادي أو الاجتماعي، مما يؤدي إلى تبعية خاصة معروفة لدى الجاني.

وبناءً على ما سبق، نستخلص أن المشرع الفرنسي يجرم التنمر الإلكتروني، بما في ذلك التحرش الجنسي الإلكتروني أو التحرش بقاصر أو باستغلال ضعف الضحية. وبسبب خطورة هذه الأفعال، اعتبر المشرع الفرنسي هذه الجرائم مشددة للعقاب، حيث تصل عقوبة السجن إلى ثلاث سنوات بدلًا من سنتين، وزيادة الغرامة المالية إلى 45,000 يورو بدلًا من 30,000 يورو.

كما جرم المشرع الفرنسي نشر محتوى إباحي يتعلق بالقاصرين، حيث يعاقب من ينشر هذا المحتوى بالسجن لمدة تصل إلى خمس سنوات وغرامة تصل إلى 75,000 يورو.

وعلاوة على ذلك، يجرم المشرع الفرنسي التعليقات أو السلوكيات المتكررة التي تشكل تحرشًا جنسيًا ضمن نطاق التنمر الإلكتروني، والمعروفة بالغارات الرقمية، ويعاقب عليها ضمن إطار الجرائم الإلكترونية[1].

بالإضافة إلى ذلك– وفقًا للتعديلات الصادرة في عام 2018، يجرم المشرع الفرنسي أفعال الازدراء الجنسي، والتي تشمل أي سلوك يهين كرامة الشخص بسبب شخصيته أو وظيفته. ويعاقب على هذه الجرائم بغرامة تتراوح بين 90 إلى 750 يورو، وتصل العقوبة إلى غرامة تتراوح بين 1,500 إلى 3,000 يورو إذا وقعت الجريمة على قاصر دون الخامسة عشرة، أو شخص ضعيف أو في وضع غير مستقر، أو في وسائل النقل العام، أو بسبب التوجه الجنسي.

وانطلاقًا مما سبق، يتضح أن المشرع الفرنسي قد اتخذ خطوات جديدة لحماية القاصرين من الجرائم الجنسية والتحرش الجنسي بجميع أشكاله، بما في ذلك التحرش الإلكتروني. ووفقًا للتعديلات الجديدة في قانون العقوبات الفرنسي بموجب القانون رقم 703 لسنة 2018، الصادر في 3 أغسطس 2018، تم إدخال مجموعة من القواعد القانونية الجديدة، وهي كالتالي:

- **أولًا:** تم تمديد فترة التقادم للجرائم الجنسية المرتكبة ضد القاصرين من 20 عامًا إلى 30 عامًا، بحيث يبدأ حساب هذه الفترة من تاريخ انتهاء السلوك الإجرامي.

---

[1] AJ FAM, Loi sur les violences sexistes et sexuelles, Dalloz, Paris, 2018, P. 422.

- **ثانيًا:** في حالة الاعتداء الجنسي على قاصر، يفترض المشرع الفرنسي وقوع الاعتداء بالإكراه، حتى في حالة موافقة القاصر، وهذا الافتراض لا يقبل الطعن.
- **ثالثًا:** أثيرت تساؤلات حول دستورية هذا التعديل، إلا أن المجلس الدستوري الفرنسي أكد دستوريته وفقًا لمفهوم الرقابة الدستورية السابقة واللاحقة في فرنسا.
- **رابعًا:** أدخل المشرع الفرنسي جرائم جديدة تتعلق بعدم مساعدة شخص في خطر من التعرض للإيذاء الجنسي أو الاعتداء الجنسي، وكذلك عدم الإبلاغ عن مثل هذه الجرائم، بشرط أن يكون المجني عليه قاصرًا لم يتجاوز عمره 15 عامًا. وتعتبر هذه الجرائم مستمرة، ولا يبدأ حساب فترة التقادم إلا بعد انتهاء حالة الاستمرار للجريمة[1].

أما بالنسبة لموقف المشرع المصري، فقد نصت المادة 116 مكرر (أ) من قانون الطفل المصري رقم 126 لسنة 2008 على أنه[2]: "يعاقب بالحبس لمدة لا تقل عن سنتين وبغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز خمسين ألف جنيه كل من استخدم الحاسب الآلي أو الإنترنت أو شبكات المعلومات أو الرسوم المتحركة لإعداد أو حفظ أو معالجة أو عرض أو طباعة أو نشر أو ترويج أنشطة أو أعمال إباحية تتعلق بتحريض الأطفال أو استغلالهم في الدعارة أو الأعمال الإباحية أو التشهير بهم أو بيعهم. كما يُعاقب بذات العقوبة كل من استخدم الوسائل السابقة لتحريض الأطفال على الانحراف أو تسخيرهم في ارتكاب الجرائم أو في القيام بأنشطة أو أعمال غير مشروعة أو منافية للآداب، حتى وإن لم تقع الجريمة فعلًا".

كما نصت المادة 116 مكررًا (ب) من ذات القانون على أنه: "مع عدم الإخلال بأي عقوبة أشد ينص عليها قانون آخر، يُعاقب بغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز خمسين ألف جنيه كل من نشر أو أذاع من خلال أحد أجهزة الإعلام أي معلومات أو بيانات، أو أي رسوم أو صور تتعلق بهوية الطفل عند عرض قضيته على الجهات المختصة بالأطفال المعرضين للخطر أو المخالفين للقانون".

بالإضافة إلى ذلك، نص المشرع المصري في المادة 25 من قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018 على أنه[3]: "يعاقب بالحبس لمدة لا تقل عن ستة أشهر،

---

[1] للمزيد من التفصيل يراجع: د. ياسر محمد اللمعي، المواجهة الجنائية لظاهرة التنمر الإلكتروني في ضوء السياسة التشريعية الحديثة، مرجع سابق، ص 56-57.

[2] قانون الطفل المصري رقم 12 لسنة 1996، والمعدل بالقانون رقم 126 لسنة 2008.

[3] قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لسنة 2018، الصادر في 14 أغسطس، الجريدة الرسمية عدد 32 (ج)، ص 18.

وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من أرسل بكثافة العديد من الرسائل الإلكترونية لشخص معين دون موافقته، أو منح بيانات شخصية إلى نظام أو موقع إلكتروني لترويج السلع أو الخدمات دون موافقته، أو نشر عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات معلومات أو أخبارًا أو صورًا وما في حكمها، تنتهك خصوصية أي شخص دون رضاه، سواء كانت المعلومات المنشورة صحيحة أم غير صحيحة".

كما نص المشرع المصري في المادة (26) من ذات القانون على أنه: "يعاقب بالحبس لمدة لا تقل عن سنتين ولا تجاوز خمس سنوات، وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز ثلاثمائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من تعمد استعمال برنامج معلوماتي أو تقنية معلوماتية في معالجة معطيات شخصية للغير لربطها بمحتوى منافٍ للآداب العامة، أو لإظهارها بطريقة من شأنها المساس باعتباره أو شرفه".

ويتضح مما سبق، أن المشرع المصري قد وضع حماية ضد التحرش الإلكتروني من خلال نشر أخبار أو صور أو ملفات أخرى عبر الشبكة المعلوماتية أو أي وسيلة من وسائل تقنية المعلومات، بشرط أن يشكل هذا النشر انتهاكًا لخصوصية الشخص وأن يتم دون رضاه أو موافقته. ولا يؤثر في العقاب ما إذا كانت المعلومات المنشورة صحيحة أو غير صحيحة.

كما أن المشرع المصري يعاقب على تعمد استخدام برنامج معلوماتي أو تقنية معلوماتية لمعالجة بيانات شخصية للغير، بهدف ربطها بمحتوى منافٍ للآداب العامة أو لإظهارها بطريقة تسيء إلى سمعته أو شرفه، ويعتبر ذلك شكلًا من أشكال التنمر الإلكتروني، لا سيما التنمر الجنسي باستخدام البيانات الشخصية للمجني عليه.

ووفقًا لما تقدم، يتضح أن التشريع المصري يُعتبر الأكثر تميزًا؛ نظرًا لشمولية نطاقه، حيث يوفر تغطية قانونية واسعة تشمل كافة أشكال التحرش الإلكتروني دون تقييدها ببيئات أو علاقات محددة، مما يعزز من حماية الأفراد في مختلف البيئات الاجتماعية والتكنولوجية. وهذا يضمن أن القانون يمكن أن يتصدى لأي شكل من أشكال الإساءة أو الانتهاك الرقمي بغض النظر عن البيئة الذي يحدث فيها. كما يظهر تميز التشريع المصري في تطبيق العقوبات؛ حيث يمنح القاضي سلطة تقديرية واسعة لتحديد العقوبة الأنسب بناءً على خطورة الفعل وظروف الجاني، فتتيح هذه المرونة تكييف العقوبة بما يتناسب مع طبيعة الجريمة والملابسات المحيطة بها، مما يساهم في تحقيق العدالة الجنائية بشكل أكثر فعالية ودقة، ويضمن أن العقوبات المفروضة تعكس بحق مدى خطورة الأفعال المرتكبة وتأثيرها على الضحايا.

ثالثًا– الإزعاج والمضايقة الإلكترونية:

يقصد بالإزعاج أو المضايقة هنا استخدام أحد الأشخاص لأجهزة الاتصالات بطريقة تسبب إزعاجًا أو مضايقة للطرف الآخر، وقد جرم المشرع المصري هذا الفعل إذا وقع باستخدام أي من أجهزة الاتصالات، سواء كان ذلك عبر الهاتف المحمول، أو الحاسب الآلي، أو البريد الإلكتروني، أو الرسائل الإلكترونية، أو الإنترنت، أو الاتصال التليفوني، أو غيرها من وسائل الاتصال. فكل إزعاج أو مضايقة تتم عبر هذه الأجهزة يشكل جريمة وفقًا للفقرة الثانية من المادة 76 من قانون الاتصالات المصري رقم 10 لسنة 2003. ويعد من يرتكب هذا الفعل، كإرسال رسائل عبر شبكة الإنترنت أو الهاتف المحمول تتضمن إزعاجًا أو مضايقة للمستقبل، مرتكبًا لهذه الجريمة. ويترك للقاضي تقدير ما إذا كان الفعل يشكل إزعاجًا أو مضايقة، حيث تختلف هذه المسألة بحسب ظروف كل حالة[1].

وتأكيدًا على هذا الموقف، نص المشرع المصري في المادة 166 مكرر من قانون العقوبات على أنه: "كل من تسبب عمدًا في إزعاج غيره بإساءة استعمال أجهزة المواصلات التليفونية يُعاقب بالحبس لمدة لا تجاوز سنة وبغرامة لا تزيد على مائة جنيه أو بإحدى هاتين العقوبتين". كما نصت المادة 308 مكرر (1) و(2) من قانون العقوبات على أنه: "كل من قذف غيره بطريق التليفون يُعاقب بالعقوبات المنصوص عليها في المادة 303 من ذات القانون"[2].

بالإضافة إلى ذلك، نصت الفقرة الثانية من المادة 76 من قانون الاتصالات رقم 10 لسنة 2003 على أنه: "مع عدم الإخلال بالحق في التعويض المناسب، يُعاقب بالحبس وبغرامة لا تقل عن خمسمائة جنيه ولا تجاوز عشرين ألف جنيه أو بإحدى هاتين العقوبتين، كل من تعمد إزعاج أو مضايقة غيره بإساءة استعمال أجهزة الاتصال".

ويتضح لنا أن المشرع المصري في قانون الاتصالات قد اشترط لقيام جريمة تعمد إزعاج أو مضايقة الغير بإساءة استعمال أجهزة الاتصالات توافر ركنين أساسيين:

أولًا– الركن المادي: يتمثل هذا الركن في ارتكاب الجاني لسلوك إيجابي يُحدث إزعاجًا أو مضايقة للغير. وقد اشترط المشرع أن يتم هذا السلوك الإجرامي من خلال استخدام أجهزة الاتصالات الخاصة بالمستخدم، والتي ترتبط بشبكة اتصالات عامة أو خاصة، وذلك وفقًا

---

[1] المحكمة الاقتصادية المصرية، الحكم رقم 608 لسنة 2013، جلسة 3 أغسطس 2013.

[2] تنص المادة 303 من قانون العقوبات على أنه: "يعاقب على القذف بالحبس مدة لا تجاوز سنة وبغرامة لا تقل عن ألفين وخمسمائة جنيه ولا تزيد على سبعة آلاف وخمسمائة جنيه أو بإحدى هاتين العقوبتين".

لتعريف المشرع لأجهزة الاتصالات في الفقرة العاشرة من المادة الأولى من قانون الاتصالات. وتشترط الجريمة أن يترتب على هذا السلوك الإجرامي إحداث إزعاج أو مضايقة للغير، مع ضرورة وجود علاقة سببية بين فعل الجاني والنتيجة الإجرامية؛ بحيث إنه لولا قيام الجاني باستخدام وسيلة الاتصال على هذا النحو لما تحققت النتيجة الإجرامية المتمثلة في إزعاج أو مضايقة الغير.

ثانيًا- الركن المعنوي: تعتبر هذه الجريمة من الجرائم العمدية التي تتطلب لقيامها توافر القصد الجنائي العام بعنصريه: العلم والإرادة، حيث يجب أن يكون الجاني على علم بأنه يستخدم أجهزة الاتصالات بطريقة تؤدي إلى إزعاج أو مضايقة الغير، وأن تكون إرادته الحرة والواعية متجهة نحو تحقيق هذه النتيجة الإجرامية، أي إحداث الإزعاج أو المضايقة للغير[1].

مما سبق يتضح أن المشرع المصري قد استقر فقهًا على تجريم المعاكسات التي تقع عبر أي جهاز من أجهزة الاتصالات، سواء كان ذلك التليفون أو الحاسب الآلي أو البريد الإلكتروني أو الرسائل الإلكترونية عبر الإنترنت. فوفقًا للفقرة الثانية من المادة 76 من قانون الاتصالات، فإن أي إزعاج أو مضايقة تتم من خلال هذه الأجهزة يُعد جريمة. ويُعد من يقوم بإرسال رسائل عبر شبكة الإنترنت أو التليفون المحمول تتضمن إزعاجًا أو مضايقة لمستقبلها مرتكبًا لهذه الجريمة، ويترك للقاضي تقدير ما إذا كان الفعل يشكل إزعاجًا أو مضايقة للمتلقي، وهي مسألة موضوعية تختلف من حالة إلى أخرى[2].

ويمثل هذا الأمر إحدى صور التنمر الإلكتروني من خلال تكرار إرسال رسائل تهدف إلى إزعاج أو مضايقة المجني عليه. فقد أساء البعض استخدام إمكانات شبكة الإنترنت لارتكاب أفعال تندرج تحت طائلة قانون العقوبات، مثل المعاكسات عبر البريد الإلكتروني، فمن خلال معرفة عنوان البريد الإلكتروني، يمكن لمستخدم الشبكة إرسال رسائل تتضمن مغازلات، أو إهانات، أو رسومات مبتذلة، أو حتى شتائم، مما يُعد من الجرائم المخلة بالآداب العامة أو المساس بالاعتبار والشرف، كما في جرائم القذف والسب[3]. ويُعد تكرار هذه الأفعال ظاهرة

---

[1] د. ياسر محمد اللمعي، المواجهة الجنائية لظاهرة التنمر الإلكتروني في ضوء السياسة التشريعية الحديثة، مرجع سابق، ص 76.

[2] د. عمر الشريف، شرح مبادئ وأحكام قوانين الاتصالات، الطبعة الأولى، كلية الهندسة، جامعة الإسكندرية، 2008م، ص 124؛ م. مصطفى معوض، م. أكرم أبو حساب، الموسوعة الجنائية للتشريعات الاقتصادية، الطبعة الأولى، طبعة خاصة بنادي القضاة، القاهرة، 2009م، ج 2، ص 397.

[3] د. جميل عبد الباقي الصغير، جرائم الإنترنت: الأحكام الموضوعية والجوانب الإجرائية، طبعة خاصة بنادي القضاة، القاهرة، 2011م، ص 2 وما بعدها.

إجرامية تعرف بالتنمر الإلكتروني، وتتجلى في صورة تحرش إلكتروني أو ملاحقة أو مطاردة عبر الرسائل الإلكترونية.

وتطبيقًا لذلك، قضت محكمة النقض: "بأن جريمة تعمد إزعاج الغير باستعمال أجهزة الاتصالات تتحقق عند ثبوت تكرار الاتصال بالضحية لفترة طويلة واستخدام ألفاظ مسيئة. وفي حكمها، أكدت المحكمة على اطمئنانها إلى أقوال المجني عليه وما أثبته محرر محضر الضبط من معاينة أجهزة التليفون الخاصة بالمجني عليه، والتي أظهرت تعمد الطاعن إزعاج المجني عليه بإساءة استعمال أجهزة الاتصال المملوكة له، بتكرار الاتصال به على تليفوناته الخاصة لمدة تقارب العام والتعدي عليه بألفاظ نابية. وبناءً على ذلك، وجدت المحكمة أن أركان الجريمة قد تحققت، مما يجعل النعي على الحكم بالقصور في التسبيب غير وارد"[1].

كما قضت محكمة جنح طنطا الاقتصادية في 30 أغسطس 2018 بمعاقبة المتهم بالحبس لمدة ستة أشهر مع الشغل، وألزمته بدفع مبلغ ألف جنيه ككفالة لإيقاف التنفيذ، بالإضافة إلى تغريمه مبلغ عشرة آلاف جنيه عن جريمة إزعاج ومضايقة المجني عليه عبر إساءة استعمال أجهزة الاتصالات، حيث قام المتهم بإرسال رسائل من هاتفه إلى المجني عليه تضمنت ألفاظ سب تُخدش الشرف والاعتبار، بالإضافة إلى السب بطريق التليفون. وقد استند الحكم إلى نص الفقرة الثانية من المادة 76 من قانون الاتصالات رقم 10 لسنة 2003، والمواد 166 مكررًا، 306، 308 مكررًا (1) و(2) من قانون العقوبات، وذلك تطبيقًا لنص المادة 304 الفقرة الثانية من قانون الإجراءات الجنائية[2].

وقد استند الحكم إلى أن الدليل قد توافر على صحة الجريمة الأولى، وهي أن المتهم تعمد إزعاج ومضايقة المجني عليه بإساءة استعمال أجهزة الاتصالات عبر إرسال رسائل تشمل ألفاظ سب تخدش الشرف والاعتبار، مما ضاق بها صدر المجني عليه، وهو ما يحقق الركن المادي لهذه الجريمة. كما ثبت علم المتهم بإساءة استعمال جهاز الاتصال المذكور في إرسال تلك الرسائل الإلكترونية للمجني عليه بهدف إزعاجه ومضايقته، مما يحقق الركن المعنوي للجريمة.

كذلك، ثبت الدليل على صحة الجريمة الثانية التي تتعلق بقيام المتهم بسب المجني عليه بطريق التليفون، وذلك بعلم بأن تلك الرسائل تتضمن خدشًا للشرف والاعتبار، مع اتجاه إرادته لتحقيق هذا الفعل، مما يحقق ركني الجريمة المادي والمعنوي.

---

[1] محكمة النقض المصرية، نقض جنائي، الطعن رقم 1194 لسنة 80 ق، جلسة 14 مارس 2011م.

[2] محكمة جنح طنطا الاقتصادية، الدائرة الثالثة الابتدائية، قضية النيابة العامة رقم 1099 لسنة 2018، جلسة 30 أغسطس 2018؛ وكذلك حكم المحكمة الاقتصادية رقم 471 لسنة 2012، جلسة 19 نوفمبر 2012م.

ومن المقرر أن الإزعاج، وفقًا لنص المادة 166 مكررًا من قانون العقوبات، لا يقتصر على السب والقذف، حيث إن المشرع قد تناول هذه الجرائم في المادة 308 مكررًا، بل يتسع ليشمل كل قول أو فعل تعمده الجاني ويؤدي إلى تضييق صدر المواطن. وفي هذا السياق، إذا لم يبين الحكم المطعون فيه الأفعال أو الأقوال التي صدرت من الطاعن وتعد إزعاجًا، وكيفية اعتبار اتصال الطاعن بالشخصيات العامة لطلب توصيات منهم لقضاء مصالح شخصية إزعاجًا لهم، باعتبار أن هذه الجريمة من الجرائم العمدية، ولم يوضح مؤدى أقوال المجني عليهم أو مضمون تقرير خبير الأصوات للاستدلال بها على ثبوت التهمة، فإن الحكم يكون معيبًا بالقصور[1].

وبذلك، أكد المشرع المصري على تجريم أي سلوك يهدف إلى إزعاج أو مضايقة الغير إذا تم عبر أجهزة الاتصالات، سواء كان ذلك باستخدام الهاتف المحمول، أو الحاسب الآلي، أو البريد الإلكتروني، أو أي وسيلة إلكترونية أخرى، ويُعد هذا التجريم شاملًا لجميع أشكال الإساءة التي تُرتكب باستخدام هذه الوسائل. ويتجلى من هذا التشريع حرص المشرع على حماية كرامة الأفراد واعتبارهم الشخصي من أي اعتداء عبر الوسائل الإلكترونية، من خلال تجريم الأفعال التي تنطوي على سب أو قذف أو إساءة استخدام لأجهزة الاتصالات، بما يضمن صيانة الحقوق الشخصية وحمايتها من الإهانة أو التهديد.

أما بالنسبة لموقف المشرع الفرنسي من الإزعاج والمضايقات الإلكترونية، فقد نصت المادة 222–33–2 من قانون العقوبات الفرنسي على أنه: "يُعاقب بالسجن لمدة لا تزيد على عامين وبغرامة مالية لا تتجاوز 30,000 يورو كل من قام بمضايقة الآخرين من خلال كلام أو سلوك متكرر بشكل متعمد، مما أدى إلى تدهور ظروف العمل، أو التأثير على حقوقهم أو كرامتهم، أو تسبب في إضعاف صحتهم البدنية أو العقلية، أو هدد مستقبلهم المهني[2].

كما تنص المادة 222–33–2–1 من قانون العقوبات الفرنسي على أن مضايقة الزوج أو الشريك، سواء كان شريكًا وفقًا لرابطة الميثاق المدنية أو شريكًا بالمعاشرة، والتي يكون الغرض منها أو ينتج عنها تدهور في ظروف المعيشة يؤدي إلى إضعاف الصحة الجسدية أو العقلية، يُعاقب عليها بالسجن لمدة لا تزيد على ثلاث سنوات وبغرامة مالية لا تتجاوز 45,000 يورو،

---

[1] محكمة النقض المصرية، نقض جنائي، الطعن رقم 25065 لسنة 59 ق، جلسة 1 يناير 1995م، س 46، ق 1، ص 24.

[2] المادة 222–33–2 من قانون العقوبات الفرنسي، والمعدلة بموجب المادة 40 من القانون رقم 873 لسنة 2014، الصادر في 4 أغسطس 2014.

وذلك بشرط أن تكون هذه الأفعال قد تسببت في عجز كلي عن العمل لمدة لا تزيد على ثمانية أيام.

وتُشدد العقوبة لتصبح السجن لمدة لا تزيد على خمس سنوات وبغرامة مالية لا تتجاوز 75,000 يورو إذا تسببت هذه الأفعال في عجز كلي عن العمل لمدة تتجاوز ثمانية أيام، أو إذا ارتكبت تلك الأفعال في حضور قاصر. وتُطبق نفس العقوبات عندما يتم ارتكاب الأفعال المذكورة من قبل زوج سابق أو شريك سابق كان مرتبطًا بالمجني عليه بموجب ميثاق مدني.

وفي ذلك قضت محكمة استئناف باريس في 13 أبريل 2016 بأن كل فعل من شأنه تهديد سمعة الضحية بخطر يُعد نوعًا من التنمر الإلكتروني، والذي يتخذ صورة البلطجة أو التسلط الإلكتروني[1]، دون الحاجة إلى ذكر التفاصيل، ويعتبر ذلك شكلًا من أشكال التحرش الإلكتروني من قبل الشريك المعاشر السابق[2]. وفي هذا السياق، عوقبت امرأة بالسجن بسبب استخدامها وسائل تكنولوجية لإهانة وتهديد زوجها السابق وعشيقته، حيث قامت المتهمة بإخفاء هويتها واستخدام عشرة أسماء مستعارة على شبكات التواصل الاجتماعي، بما في ذلك فيسبوك، لنشر صور خاصة بزوجها السابق بهدف تشويه سمعته في مكان عمله. وفيما يتعلق بعشيقته، أرسلت المتهمة العديد من الرسائل الإلكترونية غير المرغوب فيها التي تضمنت مشاعر الكراهية والحقد. وقد تم التحفظ على هذه الأدلة الإلكترونية الجنائية كوسيلة لإثبات ارتكاب الجريمة. وبناءً على

(1) Crim. 16 mars 2016, n° 15-82.676, Dalloz, 2016, P. 935., note A. SERINET, Le consentement et la répression de la diffusion d'une image intime, Recueil Dalloz, 2016 p.935. 1597, chron. B. Laurent, L. Ascensi, E. Pichon et G. Guého, Chronique de jurisprudence de la Cour de cassation, AJ pénal 2016, P. 268, obs. J.-B. Thierry; Dalloz IP/IT 2016, P. 321, obs. G. Desgens-Pasanau; Rev. Sin. Crim, 2016, P. 96, obs. J. Francillon; CCE 2016, comm. n° 42, note A. Lepage; JCP 2016, P. 658, note J.-C. Saint-Pau.

(2) Usurpation de l'identité numérique d'un tiers (C. pén., art. 226-4-1, al. 1 et 2), harcèlement par concubin (C. pén., art. 222-33-2-1), atteinte à la représentation de la personne (C. pén., art. 226-8), agressions sonores (C. pén., art. 222-16), violences volontaires avec préméditation (C. pén., art. 222-11 et 222-12, al. 1, 9°).

ذلك، تمت الإدانة استنادًا إلى استخدام شبكات الاتصال العامة عبر الإنترنت لتقويض شرف شخص وعشيقته، مما أدى إلى وقوع ضرر جسيم بسمعتهما[1].

ويتضح مما سبق أن المشرع الفرنسي قد وضع إطارًا قانونيًا صارمًا لمكافحة الإزعاج والمضايقات الإلكترونية، مستهدفًا حماية كرامة الأفراد وصحتهم الجسدية والعقلية، وكذلك حقوقهم الشخصية والمهنية. فيعاقب القانون على السلوك المتكرر والمتعمد الذي يتم عبر الوسائل الإلكترونية ويؤدي إلى إزعاج أو مضايقة الغير، مما يهدد حقوق الشخص أو سمعته. كما تُشدد العقوبات في الحالات التي تشمل العنف المنزلي أو استهداف القاصرين. وأقر المشرع أيضًا بأهمية استخدام الأدلة الإلكترونية كوسيلة فعالة لإثبات الجرائم المرتبطة بالإزعاج والمضايقات الإلكترونية، مما يعكس التزام القضاء الفرنسي بتحقيق العدالة في ظل التحديات التكنولوجية الحديثة وحماية الأفراد من أي اعتداءات تمس كرامتهم أو حقوقهم عبر الوسائل الرقمية.

رابعًا- الاعتداء على الحق في الصورة:

إن تصوير ضحايا الحوادث ونشرها على مواقع التواصل الاجتماعي بقصد التباهي أصبح ظاهرة تستدعي تدخلًا تشريعيًا عاجلًا لمواجهتها. وبالمثل، فإن التقاط الصور غير اللائقة أو المهينة لشخص ونشرها عبر منصات التواصل الاجتماعي دون موافقته يشكل نوعًا من أنواع التنمر الإلكتروني، وذلك باستخدام الإنترنت وتقنيات المعلومات بهدف إلحاق الضرر بالآخرين بأسلوب عدائي متعمد، ومتكرر[2]. لذا، يتعين على المشرع التدخل لوضع نصوص قانونية صريحة تهدف إلى مكافحة هذه الظاهرة الإجرامية لما تشكله من خطورة جسيمة على المجتمع؛ حيث تساهم في نشر الشائعات، والأقاويل الملفقة، والصور المضللة على منصات التواصل الاجتماعي ومواقع الإنترنت المختلفة، مما يؤدي إلى زعزعة الاستقرار الاجتماعي.

وفيما يتعلق بموقف المشرع الفرنسي، نجد أنه قد نصّ في المادة 368 من قانون العقوبات الفرنسي القديم على تجريم التعدي على الحق في الصورة، وقد استمر العمل بهذه المادة دون تعديل في المواد 226-1 و226-2 من قانون العقوبات الفرنسي الحالي. ويشترط لتطبيق هذه المواد أن يتم التقاط الصورة في مكان خاص دون رضى المجني عليه[3]. حيث نصت هذه

---

(1) V. En ce sens les textes de l'art. 226-4-1, al. 2 C. pén. incriminant l'usurpation de l'identité numérique d'un tiers.

(2) أ. خولة مرتضوي، ريشة حبر، بلاتينيوم بوك للنشر والتوزيع، قطر، 2016م، ص 113-114.

(3) Michele - Laure RASST, Droit pénal special, éd., Dalloz, Paris, 1997, p. 369.

المواد على تجريم فعل التقاط أو تسجيل أو نقل صورة لشخص في مكان خاص دون موافقته، مقررة عقوبة الحبس لمدة لا تتجاوز سنة واحدة، وغرامة مالية لا تتجاوز 45,000 يورو.

كما نصت المادة 226-2 من قانون العقوبات الفرنسي على معاقبة كل من يقوم بأي وسيلة بارتكاب أفعال تتعلق بجريمة الاحتفاظ أو الإعلان أو استخدام تسجيل أو مستند تم الحصول عليه من خلال الأفعال المذكورة في المادة السابقة بنفس العقوبات المنصوص عليها فيها. وعلاوة على ذلك، جرم المشرع الفرنسي أي فعل من شأنه نشر أو تركيب الصوت أو الصورة لشخص دون رضاه، وفقًا لنص المادة 226-8 من قانون العقوبات الفرنسي.

وتطبيقًا على ذلك، فقد قضت محكمة السين الفرنسية[1]: بأن الحق في الصورة هو حق لكل شخص في صورته وملامحه، ويخول له هذا الحق منع الغير من نشر صورته، وإلا كان ذلك خطأ يستوجب التعويض[2]. وفي حكم آخر، أوردت المحكمة أن للشخص الذي التُقطت صورته حق ملكية عليها، مما يمنع الآخرين من استخدامها دون موافقته. ومن هنا يمكن تشبيه الحق في الصورة بحق الملكية، خاصة من الجانب المادي.

وفي تطبيق آخر، قضت المحكمة الجنائية الفرنسية في 16 مارس 2016 بالإدانة في حالة انتهاك الحق في خصوصية الصورة، وفقًا لما نصت عليه المواد 226-1 و226-2 من قانون العقوبات الفرنسي، ولكن في ضوء تفسير ضيق لهما؛ حيث تجرم المادة الأولى انتهاك خصوصية الآخرين في الصورة عبر التقاط أو تسجيل صورة دون موافقتهم في مكان خاص[3]، فيما تجرم المادة الثانية الاحتفاظ بالصورة أو تركها متاحة للجمهور أو لطرف ثالث، وهي الحالة التي وقعت في القضية المذكورة، حيث قام الجاني بنشر صور لصديقته السابقة وهي في حالة

---

[1] محكمة السين الابتدائية الفرنسية، حكم بتاريخ 10 فبراير 1905م؛ ويراجع: د. نعيم عطية، حرمة الحياة الخاصة في القانونين المصري والفرنسي، مجلة العلوم الإدارية، المعهد الدولي للعلوم الإدارية، الشعبة المصرية، السنة 23، االمجلد 22، العدد الأول، القاهرة، يونية 1980م، ص 77؛ ويراجع كذلك: د. سعيد جبر، الحق في الصورة، دار النهضة العربية، القاهرة، 1986م، ص 107.

[2] Cass. Civ, 5 Novembre 1996, N°94-14798, Publié au Bulletin, Paris, p. 265.

[3] rim March 16, 2016 No. 15-82.676 Legalis.net March 17، 2016 ،Legipresse No. 337 of March 17، 2016. Pour une autre forme de cyber- harcèlement, V. TGI Paris, ord. réf., 29 mars 2016, Nathalie X. et Philippe Y.c / Emeric Z., Legalis.net, 1er avr. 2016: diffusion répétée de 34 articles nuisant à la réputation d'un couple et caractérisant le délit créé par la loi du 4 août 2014 (C. pén., art. 222-33-2-2, 4°).

عري على شبكة الإنترنت دون موافقتها، وهو ما يُعرف بنوع من "الانتقام الإباحي" كإحدى صور التنمر الإلكتروني.

وفي 7 أكتوبر 2016، قام المشرع الفرنسي بإدخال تعديل على القانون رقم 1321 لسنة 2016، وذلك بإضافة المادة 226-2-1 إلى قانون العقوبات الفرنسي، فتنص هذه المادة على معاقبة كل من يبث أو ينشر كلمات أو صور ذات طبيعة جنسية، تم الحصول عليها بموافقة صريحة أو ضمنية من الشخص المعني، أو عبر إحدى الطرق المنصوص عليها في المادة 226-1 من قانون العقوبات الفرنسي، بالسجن لمدة لا تزيد عن سنتين، وبغرامة مالية لا يتجاوز مقدارها 60,000 يورو.

وعلاوة على ذلك، اعتبرت اللجنة القومية للمعلوماتية والحريات في فرنسا (CNIL) أن صورة الشخص الطبيعي، سواء كانت ثابتة أم متحركة، تُعد من البيانات الشخصية المحمية بموجب القانون، مما يجعلها مشمولة بالحماية الجنائية لخصوصية البيانات الشخصية التي تتم معالجتها إلكترونيًا. ويُعتبر نشرها على الأجهزة الإلكترونية أو عبر الإنترنت شكلًا من أشكال جرائم التنمر الإلكتروني[1].

كما نص المشرع الفرنسي في المادة 226-3-1 من قانون العقوبات على تجريم التقاط الصور بشكل غير محدد، وهو ما يُعرف بالتلصص عن طريق الصور، أي التقاط صور غير محتشمة دون علم أو دون موافقة الشخص المعني. وفي هذه الحالة، يعاقب الجاني بالسجن لمدة لا تزيد عن سنة واحدة، وبغرامة مالية لا يتجاوز مقدارها 15,000 يورو، وتُشدد العقوبة لتصبح السجن لمدة لا تزيد عن سنتين، والغرامة المالية التي لا يتجاوز مقدارها 30,000 يورو في الحالات التالية[2]:

- **الحالة الأولى:** إذا ارتكبت الجريمة من قبل شخص يستغل سلطته.
- **الحالة الثانية:** إذا كانت الضحية قاصرًا لم يتجاوز عمره 15 عامًا.
- **الحالة الثالثة:** إذا ارتكبت الجريمة ضد شخص ضعيف أو في وضع غير مستقر.
- **الحالة الرابعة:** إذا ارتكبت الجريمة من قبل عدة أشخاص.
- **الحالة الخامسة:** إذا ارتكبت الجريمة في وسائل النقل العام.

---

[1] د. ياسر محمد اللمعي، المواجهة الجنائية لظاهرة التنمر الإلكتروني في ضوء السياسة التشريعية الحديثة، مرجع سابق، ص 96.

[2] AJ FAM, Loi sur les violences sexistes et sexuelles, Dalloz, Paris, 2018, P. 422.

وبالنظر إلى موقف المشرع المصري، فقد نصت المادة 309 مكررًا من قانون العقوبات على توقيع العقوبة على كل من يتعدى على حرمة الحياة الخاصة للأفراد في غير الحالات التي يجيزها القانون أو دون موافقة الضحية، وذلك من خلال قيام الجاني بالتقاط أو نقل صورة لشخص من مكان خاص باستخدام أي جهاز من الأجهزة أيًا كان نوعه. بالإضافة إلى ذلك، نصت المادة 309 مكررًا (أ) على توسيع نطاق العقوبة لتشمل كل من قام بإذاعة أو تسهيل إذاعة أو استخدام، حتى ولو لم يكن علنيًا، لتسجيل أو مستند تم الحصول عليه بإحدى الطرق المحددة في المادة 309 مكرر، أو كان ذلك دون موافقة الضحية، وكذلك كل من قام بتهديد شخص بإفشاء أمر تم الحصول عليه بإحدى تلك الطرق بهدف إجبار الشخص على القيام بفعل معين أو الامتناع عنه.

وعلاوة على ذلك، فقد نصت الفقرة الثانية من المادة 2/76 من قانون الاتصالات رقم 10 لسنة 2003 على أنه مع عدم الإخلال بالحق في التعويض المناسب، يعاقب بالحبس أو بغرامة لا تقل عن خمسمائة جنيه ولا تتجاوز عشرين ألف جنيه أو بإحدى هاتين العقوبتين، كل من تعمد إزعاج أو مضايقة الغير عن طريق إساءة استخدام أجهزة الاتصالات.

وتطبيقًا لهذا المبدأ، قضت المحكمة الاقتصادية[1] بأن المحكمة، وبعد أن اطلعت على أوراق الدعوى وأحاطت بها من كافة جوانبها، وبعد أن وازنت بين أدلة الاتهام ودفاع المتهم، انتهت إلى ترجيح أدلة الاتهام. وتأكد للمحكمة يقينًا ارتكاب المتهم للجريمة الثابتة بالأوراق، وذلك دون أدنى شك، حيث قام بإنشاء صفحة على موقع التواصل الاجتماعي "فيسبوك" ونشر عليها صورة خاصة بالمجني عليها، مما ألحق بها أضرارًا وتسبب في مضايقتها، وذلك كما أثبته التقرير الفني بأن المتهم هو من أرسل الرسائل عبر الموقع الذي أنشأه. وقد اطمأنت المحكمة إلى أقوال المجني عليها وإلى التقرير الفني، مما جعلها تثبت الاتهام بحق المتهم.

وبما أن الجرائم المنسوبة إلى المتهم تقوم على فعل مادي واحد، وهو إنشاء حساب على موقع "فيسبوك" عبر شبكة المعلومات الدولية (الإنترنت) يحمل اسم المجني عليها ويتضمن صورًا شخصية لها بملابسها المنزلية الداخلية، وتعمد إزعاجها ومضايقتها من خلال إساءة استخدام وسائل الاتصال، وذلك عبر نشر صورها الشخصية بملابس داخلية على شبكة المعلومات الدولية (الإنترنت)، فإن إنكار المتهم لارتكابه هذا الفعل الإجرامي لا يؤثر على ثبوت الواقعة. ويترتب على ذلك تحقق حالة التعدد المعنوي الذي يستوجب تطبيق نص المادة 32 من قانون العقوبات ومعاقبة المتهم بالجريمة الأشد. وترى المحكمة بناءً على نص المادة 32 من

---

[1] المحكمة الاقتصادية المصرية، الطعن رقم 167 لسنة 2013، جلسة 18 يوليو 2013.

قانون العقوبات أن هناك ارتباطًا معنويًا بين نقل المتهم لصورة شخصية للمجني عليها بملابس داخلية ونشرها على شبكة المعلومات الدولية (الإنترنت) والإساءة إليها، مما يقضي بمعاقبته وفقًا للجريمة الأشد المنصوص عليها في الفقرة الثانية من المادة 76 من قانون الاتصالات رقم 10 لسنة 2003.

ونستخلص مما سبق أن القضاء المصري قد اتجه إلى حماية الحق في الصورة، مستندًا في ذلك إلى نص الفقرة الثانية من المادة 76 من قانون الاتصالات رقم 10 لسنة 2003، باعتبار أن ما قام به الجاني يُعد شكلًا من أشكال التنمر الإلكتروني، حيث استخدم صورة خاصة ذات طبيعة جنسية وقام بنشرها على شبكة المعلومات الدولية (الإنترنت) دون موافقة المجني عليها.

وأخيرًا، يمكن القول أن التشريع الفرنسي يتفوق على نظيره المصري في تجريم الاعتداء على الحق في الصورة؛ وذلك لتميزه بتحديد دقيق وشامل للجرائم المتعلقة بالتقاط ونشر الصور، حيث يفصل بين الأفعال المختلفة ويخصص لكل منها عقوبات محددة، مما يعزز الحماية القانونية بوضوح وصرامة. إضافةً إلى ذلك، تتسم العقوبات الفرنسية بقدر أكبر من التشدد، ما يعزز التأثير الردعي على الأفراد المحتملين لارتكاب هذه الجرائم. ويُضاف إلى ذلك استجابة المشرع الفرنسي المستمرة للتطورات التكنولوجية من خلال تعديل القوانين لمواجهة التحديات الحديثة، مثل "الانتقام الإباحي" والتنمر الإلكتروني، مما يعكس ديناميكية التشريع الفرنسي وقدرته على مواكبة التغيرات المستجدة بفعالية وحزم.

خامسًا- الابتزاز والتهديد الإلكتروني:

يُقصد بالتهديد أو الابتزاز الإلكتروني، وفقًا لما ورد في المادة التاسعة من نظام مكافحة جرائم المعلومات، في الملحق الثاني التابع لمشروع القانون العربي النموذجي، "كل من استخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات لتهديد شخص آخر أو ابتزازه، بقصد حمله على القيام بفعل معين أو الامتناع عنه". ويعاقب مرتكب هذا الفعل بالحبس والغرامة. وتُشدد العقوبة لتصل إلى السجن مدة لا تزيد عن عشر سنوات إذا كان التهديد يتضمن ارتكاب جناية أو جنحة أو توجيه اتهامات تنال من الشرف والاعتبار.

وبالنسبة لموقف المشرع المصري، فقد نصت المادة 309 مكررًا (أ) من قانون العقوبات على أن يُعاقب بالحبس كل من أذاع أو سهل إذاعة أو استخدم، ولو في غير علانية، تسجيلًا أو مستندًا تم الحصول عليه بإحدى الطرق المبينة في المادة السابقة، أو كان ذلك دون موافقة صاحب الشأن. كما يُعاقب بالسجن لمدة لا تزيد على خمس سنوات كل من هدّد بإفشاء أمر من

الأمور التي تم الحصول عليها بإحدى الطرق المشار إليها لحمل شخص على القيام بعمل معين أو الامتناع عنه. وتُشدد العقوبة على الموظف العام إذا ارتكب أحد الأفعال المبينة في هذه المادة بالاعتماد على سلطته الوظيفية. وفي جميع الأحوال، يُحكم بمصادرة الأجهزة وغيرها من الأدوات التي استُخدمت في ارتكاب الجريمة أو التي تم الحصول عليها منها، ويُحكم بمحو التسجيلات المتحصلة عن الجريمة أو إتلافها.

وعلاوة على ذلك، نص المشرع المصري في الفقرة الثانية من المادة 24 من قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018 على أنه: "إذا استخدم الجاني البريد الإلكتروني أو الموقع أو الحساب الخاص المصطنع في أمر يسيء إلى ما نُسب إليه، يُعاقب بالحبس لمدة لا تقل عن سنة، والغرامة التي لا تقل عن خمسين ألف جنيه ولا تتجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين". ويظهر من ذلك أن المشرع المصري يجرّم اصطناع بريد إلكتروني أو موقع أو حساب خاص ثم استخدامه في أفعال تسيء إلى ما نُسب إليه، مثل استخدامه في التهديد أو الابتزاز الإلكتروني أو ارتكاب أي فعل آخر بشرط أن يترتب عليه إساءة لصاحب الشأن.

كما نص المشرع المصري في المادة 309 مكررًا (ب) المضافة بموجب القانون رقم 189 لسنة 2020 بتاريخ 5 سبتمبر 2020 على تجريم كل تهديد أو ابتزاز يُقصد به استغلال ضعف المجني عليه أو استغلال حالة يعتقد الجاني أنها تمسّ المجني عليه، مثل الجنس أو العرق أو الدين أو الأوصاف البدنية أو الحالة الصحية أو العقلية أو المستوى الاجتماعي، بقصد تخويفه أو وضعه موضع السخرية أو الحط من شأنه أو إقصائه من محيطه الاجتماعي.

وبذلك، هدف المشرع المصري إلى حماية الخصوصية الشخصية من أي اعتداءات غير مشروعة؛ فقد جرم المشرع المصري في المادة 309 مكررًا (أ) من قانون العقوبات كل فعل يهدف إلى إذاعة أو استخدام تسجيلات أو مستندات تم الحصول عليها دون موافقة صاحبها، وتشدد العقوبة في حال استخدام تلك المواد للتهديد أو الابتزاز، لا سيما إذا ارتكبها موظف عام مستغلًا سلطته الوظيفية. كما وسع المشرع نطاق الحماية في قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018؛ حيث جرم اصطناع بريد إلكتروني أو موقع أو حساب خاص واستخدامه للإساءة إلى الشخص المعني، مقررًا عقوبات صارمة تشمل الحبس والغرامة. إضافة إلى ذلك، شدد القانون رقم 189 لسنة 2020 على تجريم كل تهديد أو ابتزاز يستغل ضعف المجني عليه أو أوصافه الشخصية، بهدف الإذلال أو الحط من كرامته أو إقصائه من محيطه الاجتماعي، مما يعكس التزام المشرع المصري بحماية الكرامة الإنسانية في جميع جوانبها.

أما فيما يتعلق بموقف المشرع الفرنسي، فقد نص على تجريم إفشاء سرية البيانات المرسلة في المادة 226-15 من قانون العقوبات، المعدلة بموجب القانون رقم 1168 لسنة 2013 في المادة 23 منه، على أن كل إفشاء للبيانات المرسلة بسوء نية من خلال فتح أو حذف أو تأخير أو تحويل المراسلات الموجهة إلى شخص معين أو موجهة إلى طرف آخر، أو إذا تم التوصل إلى معرفة الأسرار عن طريق الاحتيال، يُعاقب مرتكبه بالحبس لمدة لا تزيد عن سنة واحدة، وبغرامة مالية لا تتجاوز 45,000 يورو. وتُطبق ذات العقوبة على كل من تمكن بسوء نية من الكشف عن بيانات أو معلومات سرية عن طريق تحويل أو استخدام أو تركيب أجهزة إلكترونية تسهل تحقيق هذا الغرض.

وتطبيقًا لذلك، قضت محكمة النقض الفرنسية في قضية "Nikon" في أكتوبر 2001 بأن البريد الإلكتروني يُعد من المراسلات الخاصة التي تتمتع بالحماية القانونية للخصوصية، وبالتالي يخضع للأحكام المتعلقة بسرية المراسلات التي تحظر على غير المرسل إليه الاطلاع عليها أو التعرف على محتواها[1]. وبناءً على ذلك، فإن أي إفشاء لمضمون هذه الرسائل أو نشرها يُعتبر انتهاكًا لحق الفرد في خصوصية البيانات الشخصية الإلكترونية، كما يُعد استغلال هذه البيانات لأغراض التهديد أو الابتزاز نوعًا من التنمر الإلكتروني.

وبذلك، تُكرّس هذه النصوص حماية سرية البيانات الشخصية والمراسلات الإلكترونية. فقد جرم المشرع الفرنسي في المادة 226-15 من قانون العقوبات كل إفشاء بسوء نية للبيانات المرسلة أو الكشف عن الأسرار الشخصية بوسائل احتيالية، مفرضًا عقوبات صارمة تشمل الحبس والغرامة. وقد أكدت محكمة النقض الفرنسية في حكمها الصادر في قضية "Nikon" على اعتبار البريد الإلكتروني جزءًا من المراسلات الخاصة التي تتمتع بحماية قانونية صارمة للخصوصية، حيث يُعد أي إفشاء أو نشر لمحتوى هذه الرسائل انتهاكًا لحق الفرد في الخصوصية، ويُعتبر استغلالها لأغراض التهديد أو الابتزاز صورة من صور التنمر الإلكتروني، مما يعكس حرص المشرع الفرنسي على صون حرمة الحياة الشخصية في العصر الرقمي.

وهديًا على ما تقدم، يمكن القول إن التشريع المصري يتفوق في تجريم الابتزاز الإلكتروني؛ نظرًا لاتساع نطاق التجريم الذي يشمل جميع الوسائل المستخدمة في التهديد أو الابتزاز، مما يوفر حماية قانونية شاملة ومفصلة. كما أن تشديد العقوبات، التي تصل إلى السجن لخمس

---

[1] M. CAHEN, Que deviennent les emails, les comptes Webmail et les sites web après un décès? A qui appartiennent – ils ? Rentrent-ils dans la succession?; Paris, 2013, p. 2. **www.murielle-cahen.com**.

سنوات، خاصة في حالات استغلال السلطة الوظيفية، يعكس نهجًا صارمًا لردع هذه الجرائم. علاوة على ذلك، يُظهر المشرع المصري مرونة تشريعية من خلال التحديث المستمر للقوانين لمواجهة الابتزاز الإلكتروني في مختلف صوره، بما في ذلك التمييز، مما يعزز الحماية في مجتمع دائم التطور. وفي المقابل، يتميز التشريع الفرنسي بدقة تحديد الجرائم وعقوباتها، خصوصًا في مجال حماية سرية المراسلات، لكنه قد يكون أقل شمولية من حيث التطبيق مقارنة بالتشريع المصري.

المطلب الثاني

وسائل الضبط الإداري الإلكتروني في مواجهة التنمر الإلكتروني

إن مواجهة الجرائم الإلكترونية من قِبَل سلطات الضبط الإداري تعد مهمة بالغة التعقيد، ولا يمكن أن تُنفَّذ على الوجه الأكمل إلا إذا كانت هذه السلطات مجهزة بالأدوات والوسائل التي تمكنها من أداء تلك المهمة بشكل يحقق الهدف المنشود، وبما يضمن أن تكون هذه الإجراءات مشروعة ومتوافقة مع القواعد المنظمة لحقوق الإنسان وحرياته. كما يجب على هذه السلطات أن تلتزم بالواجبات الموكلة إليها بموجب القوانين والأنظمة والتعليمات السارية، دون الإخلال بهذه الواجبات أو تجاوز حدودها.

ولا تختلف وسائل الضبط الإداري الإلكتروني في طبيعتها وضوابط مشروعية استخدامها عن تلك المعتمدة في الضبط الإداري التقليدي؛ إذ تحتل لوائح الضبط الإداري الإلكتروني الصدارة في هذا المجال، يليها القرارات الفردية المستقلة الصادرة عن السلطات المختصة، وأخيرًا يأتي التنفيذ المباشر كأداة فعّالة في مواجهة حالات التنمر الإلكتروني[1].

ومن الضروري أن تكون الوسائل التي تعتمدها سلطات الضبط الإداري في مكافحة التنمر الإلكتروني وفقًا لضوابط مشروعية القرارات الضبطية، والتي تم تحديدها واستقرارها من خلال اجتهادات القضاء الإداري، ويتعين أن تكون تلك الوسائل متوافقة تمامًا مع المبادئ القانونية

---

[1] للمزيد من التفصيل حول وسائل الضبط الإداري يراجع: د. مهند قاسم زغير، السلطة التقديرية للإدارة في مجال الضبط الإداري في الظروف العادية: دراسة مقارنة في القانون الوضعي والشريعة الإسلامية، رسالة دكتوراة، كلية الحقوق، جامعة النهرين، بغداد، 2014م، ص 125 وما بعدها، منشورة على الموقع الآتي: https://nahrainuniv.edu.iq/sites/default/files/nwee%20old.pdf؛ أ. عمر بو قريط، الرقابة القضائية على تدابير الضبط الإداري، مرجع سابق، ص 43 وما بعدها.

الراسخة التي تحكم ممارسة السلطة الإدارية، بما يضمن تحقيق التوازن بين الحفاظ على النظام العام وحماية حقوق الأفراد وحرياتهم الأساسية، دون تجاوز أو إساءة استخدام لهذه السلطات[1].

أولًا- لوائح الضبط الإداري الإلكتروني:

تُعدّ لوائح الضبط الإداري الإلكتروني من أهم الأدوات التي تعتمدها سلطات الضبط الإداري في مواجهة التنمر الإلكتروني، حيث تصدر هذه اللوائح عن السلطة التنفيذية بقصد الحفاظ على النظام العام بعناصره المختلفة. وتكتسب وظيفة الضبط الإداري أهمية بالغة كونها ضرورة اجتماعية لا غنى عنها في أي مجتمع، إذ إن الوقاية من الأضرار والجرائم يُعدّ أكثر فعالية من معالجتها بعد وقوعها. وتبرز لوائح الضبط الإداري الإلكتروني كأبرز مظاهر ممارسة السلطة الإدارية؛ حيث تتضمن وضع قواعد عامة وموضوعية مجردة تُقيد من خلالها أنشطة الأفراد بهدف صيانة النظام العام في الفضاء الإلكتروني، ومن الطبيعي أن تمس هذه اللوائح حقوق الأفراد وتُقيّد حرياتهم، إذ تتضمن أوامر أو نواهي، وتفرض في كثير من الأحيان عقوبات على مخالفيها[2].

وبموجب سلطات الضبط الإداري الإلكتروني في مواجهة التنمر الإلكتروني، يجري تضمين اللوائح التنظيمية تدابير وإجراءات تشكل قيودًا على الحقوق والحريات الرقمية والأنشطة المكفولة دستوريًا، ومن أبرز هذه التدابير حظر الأنشطة الرقمية التي تشكل خطرًا على النظام العام، أو اشتراط الحصول على ترخيص مسبق لمزاولة أنشطة رقمية معينة، أو رهن مشروعية الاستمرار

---

[1] يميل غالبية الفقهاء في مصر إلى أن رقابة القاضي الإداري على مشروعية قرارات الضبط الإداري لا تقتصر على مجرد فحص مدى مشروعية تلك القرارات، بل تمتد لتشمل أيضًا تقييم مدى ملاءمتها كعنصر من عناصر المشروعية. للمزيد من التفصيل حول موقف الفقه من هذه المسألة يراجع: د. سامي جمال الدين، قضاء الملاءمة والسلطة التقديرية للإدارة، دار النهضة العربية، القاهرة، 1992م، ص 218 وما بعدها؛ د. سليمان محمد الطماوي، النظرية العامة للقرارات الإدارية: دراسة مقارنة، دار الفكر العربي، القاهرة، 1984م، ص 90 وما بعدها؛ د. طارق فتح الله خضر، دعوى الإلغاء، دار النهضة العربية، القاهرة، 2002م، ص 206 وما بعدها؛ د. رمضان محمد بطيخ، الاتجاهات المتطورة في قضاء مجلس الدولة الفرنسي للحد من سلطة الإدارة التقديرية وموقف مجلس الدولة المصري منها، دار النهضة العربية، القاهرة، 1994م، ص 185 وما بعدها؛ د. ثروت عبد العال أحمد، الرقابة القضائية على ملاءمة القرارات الإدارية، رسالة دكتوراة، كلية الحقوق، جامعة أسيوط، 1991م، ص 181 وما بعدها؛ د. محمد فريد سليمان، الرقابة القضائية على التناسب في القرار الإداري، رسالة دكتوراة، كلية الحقوق، جامعة المنصورة، 1989م، ص 411 وما بعدها.

[2] يراجع: محمد علي حسونة، حدود سلطات الضبط الإداري وأثرها على الحريات العامة، المجلة القانونية، المجلد 14، العدد 1، كلية الحقوق، جامعة القاهرة، نوفمبر 2022م، ص 168.

في مزاولة بعض الأنشطة الرقمية بإخطار الجهة الإدارية المختصة بمتابعتها، كما تشمل هذه التدابير وضع تنظيمات محددة أو إيضاحات لكيفية ممارسة بعض الأنشطة الرقمية، وهو ما سنتناوله تفصيلًا فيما يلي:

1- حظر أو منع النشاط الرقمي:

يقصد بحظر النشاط الرقمي منع ممارسة نشاط رقمي معين إما بشكل كلي أو جزئي. وتُعد القاعدة الراسخة في هذا السياق عدم جواز الحظر المطلق للأنشطة والحريات الرقمية، حيث تُعتبر هذه الحريات والأنشطة امتدادًا لفكرة النشاط والحرية الإنسانية التي لا يجوز للسلطة التشريعية أو التنفيذية المسؤولة عن تنظيم مباشرتها أن تصل بها إلى حد المصادرة، إلا إذا كان هذا النشاط غير معتبر قانونًا، بمعنى أنه لا يستحق حماية قانونية لكونه لا يمثل مصلحة مشروعة جديرة بحمايته.

وفي إطار تطبيقات الحظر أو المنع التنظيمي لسلطات الضبط الإداري الإلكتروني في مواجهة التنمر الإلكتروني، تبرز نصوص المواد 7، 8 من القانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات؛ فنصت المادة (7) على أنه: "لجهة التحقيق المختصة، متى قامت أدلة على وجود موقع يُبث من داخل الدولة أو خارجها، يحتوي على أي عبارات أو أرقام أو صور أو أفلام أو مواد دعائية أو ما في حكمها، بما يعد جريمة من الجرائم المنصوص عليها في هذا القانون، ويشكل تهديدًا للأمن القومي أو يعرض أمن البلاد أو اقتصادها القومي للخطر، أن تأمر بحجب الموقع أو المواقع التي يتم البث منها، كلما أمكن تحقيق ذلك فنيًا.

ويجب على جهة التحقيق عرض أمر الحجب على المحكمة المختصة، منعقدة في غرفة المشورة، خلال أربع وعشرين ساعة، مرفقًا بمذكرة برأيها. وتصدر المحكمة قرارها في الأمر، مُسببًا، إما بالقبول أو بالرفض، في مدة لا تتجاوز اثنتين وسبعين ساعة من وقت عرضه عليها.

ويجوز، في حالة الاستعجال لوجود خطر حالّ أو ضرر وشيك الوقوع، أن تقوم جهات التحري والضبط المختصة بإبلاغ الجهاز المختص، ليقوم بإخطار مقدم الخدمة على الفور بالحجب المؤقت للموقع أو المحتوى أو المواقع أو الروابط المذكورة في الفقرة الأولى من هذه المادة وفقًا لأحكامها. ويلتزم مقدم الخدمة بتنفيذ مضمون الإخطار فور وروده إليه.

وعلى جهة التحري والضبط التي قامت بالإبلاغ أن تحرر محضرًا تثبت فيه ما تم من إجراءات وفق أحكام الفقرة السابقة، ويُعرض المحضر على جهات التحقيق خلال ثمانٍ وأربعين ساعة من تاريخ الإبلاغ الذي وجهته للجهاز، وتتبع في شأن هذا المحضر نفس الإجراءات

المبينة في الفقرة الثانية من هذه المادة، وتصدر المحكمة المختصة قرارها في هذه الحالة إما بتأييد ما تم من إجراءات الحجب أو بوقفها.

فإذا لم يُعرض المحضر المشار إليه في الفقرة السابقة في الموعد المحدد، يُعتبر الحجب الذي تم كأن لم يكن.

ويجوز للمحكمة المختصة أثناء نظر الدعوى، أو بناءً على طلب جهة التحقيق أو الجهاز أو ذوي الشأن، أن تأمر بإنهاء القرار الصادر بالحجب أو تعديل نطاقه. وفي جميع الأحوال، يسقط القرار الصادر بالحجب بصدور أمر بألا وجه لإقامة الدعوى الجنائية، أو بصدور حكم نهائي بالبراءة".

كما جاءت المادة (8) من هذا القانون لتنظم التظلم من القرارات الصادرة في شأن طلبات حجب المواقع، فقضت بأنه: "لكل من صدر ضده قرار قضائي من المنصوص عليها في المادة (7) من هذا القانون، وكذلك للنيابة العامة، ولجهة التحقيق المختصة، ولكل ذي شأن، أن يتظلم من هذا القرار أو من إجراءات تنفيذه أمام محكمة الجنايات المختصة، بعد انقضاء سبعة أيام من تاريخ صدور الأمر أو من تاريخ تنفيذه، بحسب الأحوال. وفي حالة رفض التظلم، يحق للمتظلم التقدم بتظلم جديد بعد مرور ثلاثة أشهر من تاريخ الحكم برفض التظلم.

وفي جميع الأحوال، يُقدم التظلم بتقرير يُودع في قلم كتاب محكمة الجنايات المختصة، وعلى رئيس المحكمة أن يحدد جلسة لنظر التظلم يتم إعلان المتظلم والجهاز وكل ذي شأن بها. ويجب على المحكمة أن تفصل في التظلم خلال مدة لا تتجاوز سبعة أيام من تاريخ تقديم التقرير به".

وبذلك تتضح أهمية التدابير الوقائية مثل حجب المواقع الإلكترونية كأحد أبرز وسائل حماية المجني عليهم من التعرض للتنمر الإلكتروني؛ فالمادة 7 من القانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات، تمنح جهة التحقيق المختصة صلاحية حجب المواقع التي تشكل تهديدًا للأمن القومي أو تعرض أمن البلاد للخطر، وذلك بمجرد توفر أدلة على ارتكابها لجريمة إلكترونية. ويُعزز هذا التدبير الوقائي من خلال الضمانات القضائية التي تفرض عرض أمر الحجب على المحكمة المختصة، لضمان تحقيق التوازن بين حماية الأفراد وحقوقهم الرقمية وبين الحفاظ على الأمن القومي.

إضافةً إلى ذلك، تُعد الإجراءات المنصوص عليها في المادة 8، التي تنظم حق التظلم من قرارات الحجب، ضمانة إضافية لحقوق الأفراد، حيث يمكن للمتضررين من قرارات الحجب

اللجوء إلى القضاء لإعادة النظر في تلك القرارات. ولا تقتصر هذه الآليات على حماية الأمن القومي فحسب، بل تضمن أيضًا حماية الأشخاص من التعرض للأذى الناجم عن التنمر الإلكتروني، من خلال تعطيل الأدوات التي قد يستخدمها الجناة لإلحاق الضرر بالضحايا.

ومن الأمثلة على تطبيقات الحظر الإداري الإلكتروني أيضًا في مصر، ما ورد في المادة الحادية والأربعين من لائحة التراخيص بالمجلس الأعلى للإعلام، التي تقضي بأنه: "مع عدم الإخلال باختصاصات الجهاز القومي لتنظيم الاتصالات، يُحظر استيراد أي أجهزة ثابتة أو محمولة للبث عبر الأقمار الصناعية أو شبكة المعلومات الدولية (الإنترنت) بغير طريق الهيئة الوطنية للإعلام أو الشركة المصرية لمدينة الإنتاج الإعلامي أو الشركات المملوكة للدولة العاملة في هذا المجال، ويضع المجلس الأعلى قائمة تحدد أنواع هذه الأجهزة، يتم تحديثها سنويًا أو عند الاقتضاء".

كما جاءت أيضًا نصوص المواد 22 و23 من لائحة الجزاءات والتدابير الإدارية والمالية التي يجوز توقيعها على الجهات الخاضعة لأحكام قانون تنظيم الصحافة والإعلام، والصادرة بقرار رئيس المجلس الأعلى لتنظيم الإعلام رقم 16 لسنة 2019، حيث تقضي المادة 22 بأن عدم الالتزام بقواعد التغطية الصحفية أو الإعلامية للعمليات الحربية أو الأمنية أو الحوادث الإرهابية يُعد مخالفة تستوجب توقيع جزاء المنع من النشر أو البث، أو الحجب المؤقت للصفحة أو الباب أو البرنامج أو الموقع الإلكتروني.

كما تنص المادة 23 من ذات اللائحة على أن مخالفة ميثاق الشرف المهني، سواء كان ميثاق الشرف الصحفي أو الإعلامي، أو المعايير التي يقرها المجلس الأعلى لتنظيم الإعلام، أو الأعراف المكتوبة (الأكواد)، أو التحريض على ارتكاب جريمة جنائية، أو الاستهداف السيء لشخص أو جهة ما، تُعد مخالفة تستوجب توقيع أحد الجزاءات أو بعضها، وفقًا لما يراه المجلس الأعلى لتنظيم الإعلام، والتي تشمل: منع النشر أو البث للمادة المخالفة لفترة محددة، وحجب الموقع الإلكتروني لفترة محددة أو بصفة دائمة، أو حجب الموقع الإلكتروني الشخصي الذي يتجاوز عدد متابعيه خمسة آلاف متابع.

ومن الجدير بالذكر أن صياغة هذه اللائحة قد شابها قدر من العمومية والغموض في كثير من نصوصها؛ حيث منحت المجلس الأعلى لتنظيم الإعلام، وفي بعض الأحيان رئيس المجلس منفردًا، سلطة واسعة في تقييد الأنشطة والحريات الرقمية تحت ذريعة الحفاظ على النظام العام. ومن الأمثلة على ذلك، البند الخامس من المادة 23 المذكورة، الذي يخول المجلس صلاحية

الحجب الدائم للموقع الإلكتروني، وهو ما قد يُعد مصادرة فعلية للنشاط الرقمي ذاته، بدلًا من الاقتصار على حجب المادة المخالفة للقانون[1].

ولقد انتهجت المحكمة الدستورية العليا نهجًا تقدميًا في توسيع نطاق الحماية الدستورية ليشمل عدم جواز الحظر المطلق للأنشطة والحريات الرقمية، مؤكدةً على أنه: "ثَمَّةَ مناطقُ في الحياةِ الخاصةِ لكلِّ فردٍ تمثِّلُ أغوارًا لا يجوزُ النفاذُ إليها، ويجبُ دومًا، ولِاعتبارٍ مشروعٍ، ألا يَقتحِمَها أحدٌ ضمانًا لسريَّتِها، وصَوْنًا لحرمتها، ودفعًا لأيِّ محاولةٍ للتلصصِ عليها أو اختلاسِ بعضِ جوانبها. ويُعتَبَرُ هذا الأمرُ ذا أهميةٍ خاصةٍ في ظلِّ التطورِ العلميِّ الهائلِ الذي شهدتْهُ الوسائلُ التقنيةُ الحديثة، والتي بلغَتْ في قدرتِها على الاختراقِ حدًّا مذهلًا، ممَّا كان له أثرٌ بعيدٌ على الناسِ جميعِهم، حتى في أدقِّ شؤونهم، وما يتَّصلُ بملامحِ حياتِهم، بل وببياناتِهم الشخصية التي باتَ الاطلاعُ عليها وتجميعُها نهبًا لأعينِ تلكَ الوسائلِ وآذانِها. وكثيرًا ما تسببَ النفاذُ إليها في إحراجٍ أو ضررٍ لأصحابِها. وتصونُ هذه المناطقُ من خواصِّ الحياةِ ودخائلِها مصلحتينِ قد تبدوانِ منفصلتين، إلا أنهما تتكاملان؛ إذ تتعلقانِ بوجهٍ عامٍ بنطاقِ المسائلِ الشخصيةِ التي ينبغي كتمانُها، وكذلك نطاقِ استقلالِ كلِّ فردٍ ببعضِ قراراتِه الهامَّةِ التي تكونُ- بالنظر إلى خصائصها وآثارها- أكثرَ اتصالًا بمصيرِه وتأثيرًا في أوضاعِ الحياةِ التي اختار أنماطَها. وتبلورُ هذه المناطقُ جميعَها- التي يلوذُ الفردُ بها، مطمئنًا إلى حرمتها ليهجعَ إليها بعيدًا عن أشكالِ الرقابةِ وأدواتها- الحقَّ في أن تكونَ للحياةِ الخاصةِ تخومُها التي تُرعى فيها الروابطُ الحميمةُ في نطاقِها. ولئن كانتْ بعضُ الوثائقِ الدستوريةِ لا تقررُ هذا الحقَّ بنصٍّ صريحٍ، فإن البعضَ يعتبرهُ من أشملِ الحقوقِ وأوسعِها، وهو كذلك أعمقُها اتصالًا بالقيمِ التي تدعو إليها الأممُ المتحضرةُ"[2].

كما أرست المحكمة الإدارية العليا مبدأً قضائيًا راسخًا يقضي بعدم جواز حظر الأنشطة والحريات الرقمية؛ فقد استندت المحكمة في حكمها إلى نص المادة 64 من قانون الاتصالات رقم 10 لسنة 2003م، والتي تفرض على مشغلي ومقدمي خدمات الاتصالات، وأي جهة تابعة لهم، وكذلك مستخدمي هذه الخدمات، الالتزام بعدم استخدام أية أجهزة لتشفير خدمات الاتصالات إلا بعد الحصول على الموافقة من الجهاز القومي لتنظيم الاتصالات، ومن القوات المسلحة، وأجهزة الأمن القومي. كما تؤكد المادة على ضرورة احترام حرمة الحياة الخاصة

---

[1] يراجع: د. حسين مقداد عبد اللطيف، دور الضبط الإداري في الحد من مخاطر الفضاء الإلكتروني في مصر وفرنسا، مرجع سابق، ص 727.

[2] حكم المحكمة الدستورية العليا، القضية رقم 23 لسنة 16 قضائية دستورية، جلسة 18 مارس 1995م، مجموعة أحكام المحكمة الدستورية العليا، الجزء السادس: (من أول يوليو 1993 حتى آخر يونيو 1995)، ص 567.

للمواطنين، والتي يكفلها القانون. وبموجب ذلك، يتعين على كل مشغل أو مقدم خدمة أن يتولى على نفقته الخاصة تجهيز شبكات الاتصالات المرخص له بها بكافة الإمكانات الفنية اللازمة من معدات ونظم وبرامج واتصالات، بما يتيح للقوات المسلحة وأجهزة الأمن القومي ممارسة مهامها في حدود القانون[1].

وفي حكم آخر، قضت المحكمة الإدارية العليا بأنه: "ولئن كانت التشريعات المصرية– بما فيها قانون تنظيم الاتصالات– لم تحدد بدقة الحالات التي تستدعي حجب المواقع الإلكترونية، إلا أن ذلك لا ينال من حق الأجهزة الحكومية والجهاز القومي لتنظيم الاتصالات في اتخاذ قرار بحجب بعض المواقع على الشبكة الدولية للإنترنت، إذا ما كان هناك تهديد للأمن القومي أو للمصالح العليا للدولة. ويأتي هذا الحق ضمن السلطة الممنوحة لتلك الأجهزة في مجال الضبط الإداري، وذلك لحماية النظام العام بمفهومه الثلاثي: الأمن العام، والصحة العامة، والسكينة العامة للمواطنين، على أن يكون ذلك تحت رقابة القضاء. ويتعين التفريق بين الاعتداء على الحق الفردي للأشخاص والاعتداء على المجتمع وأمنه واستقراره، وإن كان كلا النوعين من الاعتداء مرفوضًا وفقًا للشريعة والقانون والدستور. ولكن، بينما يمكن مواجهة الاعتداء على الحق الشخصي من خلال اللجوء إلى القضاء سواءً كان ذلك جنائيًا أو مدنيًا أو كلاهما معًا، وفقًا لما أشارت إليه المادة (79) من قانون تنظيم الاتصالات، فإن المساس بأمن المجتمع وأمانه لا يمكن دفعه إلا من خلال سد منبع هذا الخطر، سواء كان ذلك على شبكة الإنترنت أم غيرها، ولو بشكل مؤقت[2].

2– الإذن أو الترخيص بمزاولة النشاط الرقمي:

من أبرز الصلاحيات التي تمارسها أجهزة الضبط الإداري الإلكتروني في مواجهة التنمر الإلكتروني سلطة منح التراخيص بمزاولة الأنشطة الرقمية المختلفة، وكذلك سلطة سحب تلك التراخيص في حالة الإخلال بشروط الترخيص الممنوح مسبقًا. ويُقصد بالترخيص الضبطي، وفقًا للمادة الأولى من لائحة تنظيم التراخيص الصادرة عن المجلس الأعلى لتنظيم الإعلام، الإذن بمزاولة نشاط رقمي معين وفقًا لأحكام القانون، وذلك من خلال إصدار نموذج ترخيص ورقي أو

---

[1] حكم المحكمة الإدارية العليا، الطعن رقم 37702 لسنة 57، جلسة 24 مارس 2018.

[2] حكم المحكمة الإدارية العليا، الطعن رقم 10171 لسنة 54 ق، جلسة 26 فبراير 2012، مجموعة أحكام المحكمة الإدارية العليا، س 56، ص 877.

إلكتروني بعد استيفاء الشروط والضوابط والإجراءات المحددة في قانون تنظيم الصحافة والإعلام والمجلس الأعلى لتنظيم الإعلام واللوائح والقرارات الصادرة تنفيذًا له.

وعلى الرغم من أن الوصول إلى المجال الرقمي العام، سواء على المستوى المحلي أم العالمي، لا يتطلب عمومًا الحصول على إذن مسبق من أجهزة الضبط الإداري الإلكتروني كقاعدة عامة، فإن مزاولة بعض الأنشطة والحريات الرقمية، التي تتخذ من الفضاء الإلكتروني مجالًا لها، قد تتطلب في بعض الحالات الحصول على ترخيص مسبق من الجهة الإدارية المختصة، سواء كان المستخدم وطنيًا أم أجنبيًا.

وتتجلى أهمية الترخيص الضبطي في تنظيم وضبط الأنشطة الرقمية التي قد تنطوي على مخاطر أو تأثيرات سلبية على المجتمع، بما في ذلك الأنشطة المرتبطة بالتنمر الإلكتروني؛ حيث يشكل هذا الترخيص وسيلة أساسية لضمان الامتثال للقوانين واللوائح ذات الصلة، وحماية الأفراد من التجاوزات الرقمية التي قد تهدد حقوقهم وخصوصيتهم.

ولكن فيما يتعلق بالقرارات الصادرة عن هيئات الضبط الإداري الإلكتروني بشأن منح التراخيص، فإن هذه القرارات تخضع لرقابة القضاء، فكلما ازدادت السلطة التقديرية الممنوحة لهيئات الضبط الإداري في هذا الصدد، ازدادت رقابة القضاء عليها لضمان عدم تجاوز حدود الصلاحيات المقررة قانونًا. ويُعد الغرض الرئيسي من منح هذه التراخيص هو اتخاذ تدابير وقائية تهدف إلى حماية النظام العام من أي تهديدات أو مخاطر قد تنجم عن الأنشطة المرخصة، وذلك في إطار مواجهة ظاهرة التنمر الإلكتروني وضمان سلامة المجتمع الرقمي.

وتطبيقًا لذلك، تنص المادة 22 من لائحة تنظيم التراخيص بالمجلس الأعلى لتنظيم الإعلام على أنه: "يشترط لترخيص الوسائل الرقمية غير المصرية، سواء كانت مواقع إلكترونية أو منصات إعلامية أو إعلانية تجارية إلكترونية تقدم خدماتها داخل جمهورية مصر العربية، وكانت حاصلة على ترخيص أجنبي أو لها مركز قانوني أجنبي، وتعتزم مزاولة نشاطها الرقمي في مصر، توافر الشروط التالية: ...".

كما تنص المادة 24 من اللائحة ذاتها على أنه: "مع عدم الإخلال باختصاص الجهاز القومي لتنظيم الاتصالات في إصدار تراخيص إنشاء أو تشغيل شبكات توزيع الأقنية الفضائية (الكيبل)، يتعين على من يرغب في مزاولة نشاط توزيع الأقنية الفضائية (الكيبل) أن يتقدم بطلب إلى الأمانة العامة على النموذج المعد لهذا الغرض، مرفقًا به إيصال سداد رسم قدره مائتان وخمسون ألف جنيه مصري، أو ما يعادله بالعملة الأجنبية. وتُحيل الأمانة العامة طلبات

الترخيص إلى لجنة التراخيص المختصة، وتعد اللجنة تقريرًا برأيها بعد فحص الطلب والحصول على موافقة الجهاز القومي لتنظيم الاتصالات، ويُعرض التقرير على المجلس الأعلى للنظر في إصدار الترخيص من عدمه بعد استيفاء موافقة الأجهزة المعنية. وتكون مدة الترخيص خمس سنوات، يجوز تجديدها بناءً على طلب يقدمه المرخص له إلى المجلس الأعلى قبل ستة أشهر من انتهائه، ويتم التجديد مقابل سداد نفس الرسم المحدد في الفقرة الأولى من هذه المادة، وبعد مراجعة شروط التجديد".

وتنص المادة 13 من اللائحة المذكورة على أنه: "مع عدم الإخلال بالأحكام الواردة في القانون واللائحة التنفيذية بشأن الصحف الإلكترونية والمواقع الإلكترونية للوسائل الإعلامية، يُشترط لترخيص المواقع الإلكترونية، أو الصفحات، أو الروابط، أو التطبيقات التي تقدم الخدمات الإخبارية، أو الإعلامية، أو الإعلانية التجارية الإلكترونية، والمتضمنة الترويج للأعمال أو الخدمات أو المنتجات أو الأشخاص عبر شبكة المعلومات الدولية (الإنترنت) داخل جمهورية مصر العربية، أن يتم ذلك وفقًا لأحكام هذه اللائحة".

وتتجلى أهمية هذه الأحكام في إطار مواجهة أجهزة الضبط الإداري الإلكتروني للتنمر الإلكتروني؛ حيث تُمكن هذه الأحكام الجهات المختصة من تنظيم وضبط الأنشطة الرقمية بشكل يضمن حماية حقوق الأفراد وصون حرياتهم في الفضاء الإلكتروني، مع مراعاة المعايير القانونية اللازمة للحد من التجاوزات الرقمية وضمان أن يتم الترويج للمنتجات والخدمات ضمن إطار قانوني يحقق العدالة ويمنع إساءة الاستخدام.

بالإضافة إلى ذلك تنص المادة الخامسة والأربعون من ذات اللائحة على أن شهادة اعتماد شركات تكنولوجيا المعلومات الاجتماعية تحدد جميع الحقوق والالتزامات والاشتراطات التي يتعين على الشركة الالتزام بها، وتعتبر هذه الشروط جوهرية ولا يجوز مخالفتها بأي حال من الأحوال. ومن بين هذه الالتزامات والاشتراطات، يأتي ما يلي: ... 6. مناهضة خطاب الكراهية غير المشروع، والعمل على إرشاد المستخدمين إلى قواعد السلوك الصحيح، وزيادة وعيهم وثقافتهم، وحظر الترويج لكافة أشكال العنف أو التمييز أو العنصرية أو الكراهية.

وفي إطار مواجهة أجهزة الضبط الإداري الإلكتروني للتنمر الإلكتروني، تتجلى أهمية هذه المادة في إرساء قواعد صارمة لضبط سلوكيات المستخدمين في الفضاء الرقمي، فيتعين على شركات تكنولوجيا المعلومات الاجتماعية الالتزام بمناهضة أي محتوى ينطوي على خطاب كراهية أو ترويج للعنف أو التمييز بكافة أشكاله. كما يجب عليها توفير إرشادات واضحة

للمستخدمين حول السلوك الصحيح في الفضاء الرقمي، بما يعزز من وعيهم وثقافتهم الرقمية، ويحد من انتشار المحتويات الضارة التي قد تسهم في تفشي ظاهرة التنمر الإلكتروني.

3- الإخطار بمزاولة النشاط الرقمي:

ومعنى الإخطار السابق عن ممارسة نشاط معين أو حرية معينة، هو إخطار الإدارة المعنية للحصول على الإذن اللازم لممارسة هذا النشاط أو الحرية نظرًا لاتصالهما بالنظام العام، ويمنح هذا الإخطار هيئات الضبط الإداري صلاحية الاعتراض على النشاط في حالات معينة أو اتخاذ الاحتياطات اللازمة لمنع تهديد النظام العام. ويعني ذلك أن ممارسة النشاط الفردي مسموح بها ولا يشترط للحصول عليها إذن أو ترخيص مسبق، ولكن يتعين على الأفراد إبلاغ الإدارة المعنية عن رغبتهم في القيام بنشاط معين[1].

وفي إطار مواجهة أجهزة الضبط الإداري الإلكتروني للتنمر الإلكتروني، يتضح أن هذا الإخطار يلعب دورًا محوريًا في تنظيم الأنشطة الرقمية التي قد تتصل بالنظام العام، حيث يجب على الأفراد أو الكيانات الخاصة إخطار الجهة المعنية قبل الشروع في أي نشاط رقمي قد ينطوي على مخاطر للنظام العام. ومن ثم، تملك هذه الجهات صلاحية اتخاذ التدابير الوقائية الضرورية أو الاعتراض على النشاط إذا تطلب الأمر ذلك؛ لضمان حماية المجتمع من أي أضرار قد تنتج عن إساءة استخدام الفضاء الرقمي، خصوصًا في حالات التنمر الإلكتروني.

ومثال ذلك ما ورد في المادة 25 من لائحة التراخيص المشار إليها سابقًا، والتي تشترط أن تأخذ شركات توزيع الأقنية الفضائية (الكيبل) شكل شركة من شخص واحد أو أكثر، كما تفرض على هذه الشركات الحصول على التراخيص أو التصاريح أو الموافقات الأخرى من الجهات العامة المختصة بأعمال الإنشاء أو التركيب أو التشغيل. وتلتزم هذه الشركات بإخطار المجلس الأعلى ببيانات وموقع كل عملية إنشاء أو تشغيل خلال مدة لا تتجاوز خمسة عشر يومًا من تاريخ الانتهاء من العملية. وللمجلس الأعلى أن يتخذ الإجراءات المناسبة حيال أي مخالفات، بما في ذلك وقف الترخيص أو إلغاؤه.

---

[1] للمزيد من التفصيل يراجع: د. حلمي الدقدوقي، رقابة القضاء على المشروعية الداخلية لأعمال الضبط الإداري: دراسة مقارنة، دار المطبوعات الجامعية، الإسكندرية، 2004م، ص 175؛ د. طعيمة الجرف، القانون الإداري والمبادئ العامة في تنظيم ونشاط السلطات الإدارية، دار النهضة العربية، القاهرة، 1978م، ص 198؛ د. هاني علي الطهراوي، القانون الإداري، الكتاب الأول، الطبعة الأولى، مكتبة دار الثقافة للنشر والتوزيع، عمَّان، الأردن، 2001م، ص 244.

وتنص المادة 34 من ذات اللائحة على أنه: "يجب إبلاغ المجلس الأعلى بأي تغيير يطرأ على البيانات الواردة في طلب الترخيص لمزاولة نشاط تقديم خدمات نقل المحتوى، وذلك بكتاب مسجل مصحوب بعلم الوصول للحصول على موافقة المجلس على البيانات الجديدة. وإذا لم يوافق المجلس الأعلى على تعديل البيانات، يستمر العمل وفقًا للبيانات الأصلية، ويترتب على تعديل البيانات دون موافقة المجلس وقف الترخيص أو إلغاؤه وفقًا لتقدير المجلس".

وفي إطار تطبيق هذه الأحكام، تمثل هذه النصوص تجسيدًا للرقابة التنظيمية الصارمة التي تفرضها السلطات الإدارية على الأنشطة المرتبطة بتوزيع المحتوى الرقمي والإلكتروني، وذلك عبر آليات قانونية محكمة تهدف إلى ضمان الامتثال الكامل من قبل الشركات المعنية، بما يحفظ النظام العام ويصون حقوق الأفراد. فاشتراط الحصول على التراخيص والموافقات المسبقة، وإلزام الشركات بإخطار الجهات المختصة بأي تغييرات في بياناتها التشغيلية، يُعد تدبيرًا وقائيًا يهدف إلى تعزيز الشفافية والمساءلة. ومن خلال منح المجلس الأعلى سلطة تقديرية لاتخاذ إجراءات عقابية، مثل تعليق أو إلغاء التراخيص، يُكرَّس دور القانون كحامٍ للمجتمع من مخاطر سوء استخدام التقنيات الرقمية، بما في ذلك التنمر الإلكتروني.

4- تنظيم النشاط الرقمي:

في إطار مواجهة سلطات الضبط الإداري الإلكتروني لظاهرة التنمر الإلكتروني، قد ترى هذه السلطة أن اشتراط الحصول على إذن مسبق أو ترخيص لمزاولة نشاط رقمي معين، أو حتى الإخطار بمزاولة هذا النشاط بمجرد البدء فيه، ليس كافيًا لدرء المخاطر التي تهدد النظام العام الرقمي؛ لذلك قد تتجه السلطة إلى وضع إطار تنظيمي محدد أو كيفية مُعينة لمزاولة هذا النشاط الرقمي، بما يضمن توحيد الإجراءات وتلافي التباينات التي قد تنشأ نتيجة لاختلاف تقديرات وتوجهات الأشخاص أو الجهات المزاولة لهذا النشاط.

ويجب أن يكون تنظيم النشاط الرقمي الفردي، ضمن إطار سلطات الضبط الإداري الإلكتروني، محكومًا بمبادئ توازن دقيقة، بحيث يُفرض بأقل قدر من القيود التي تعيق النشاط، وبما يتناسب مع ضرورة المحافظة على النظام العام الرقمي. وتجدر الإشارة إلى أن هناك اتجاهًا فقهيًا يرى أن التنظيم يمثل قيدًا أشد على الحرية مقارنة بالإخطار السابق؛ وذلك لأنه يتضمن شروطًا ملزمة لا يمكن ممارسة النشاط إلا بعد استيفائها[1]. ومع ذلك، فإن الباحث يؤيد الرأي

[1] د. محمد رفعت عبد الوهاب، مبادئ وأحكام القانون الإداري، منشورات الحلبي الحقوقية، بيروت، لبنان، 2002م، ص 241.

الغالب في الفقه، والذي يرى أن هذه الصورة من التنظيم تُعد أقل تقييدًا للحريات مقارنة بالأنماط الأخرى، وبالتالي فهي تُفضل على الحظر المطلق كوسيلة لضبط الأنشطة الرقمية، خاصة في إطار مكافحة التنمر الإلكتروني.

وعلى سبيل المثال، قد تقرر سلطة الضبط الإلكتروني وضع لائحة تُحدد معايير صارمة لإنشاء وإدارة منصات التواصل الاجتماعي التي تُستخدم غالبًا في التنمر الإلكتروني، فتُلزم هذه اللائحة الجهات المشغلة بتفعيل أدوات تقنية معينة لمراقبة ورصد المحتوى المُسيء تلقائيًا، وتحديد إجراءات واضحة للاستجابة الفورية لحالات التنمر، مثل تعليق أو حظر الحسابات المسيئة. بهذا الشكل تُحكم سلطة الضبط سيطرتها على النشاط الرقمي من خلال توجيه كيفية تنفيذه وفق أسس واضحة ومحددة، مما يقلل من احتمالات حدوث تباينات في تطبيق الضوابط والتشريعات المرتبطة بمكافحة التنمر الإلكتروني.

وفيما يتعلق بإنشاء المواقع الإلكترونية الإخبارية والإعلامية والإعلانية، فقد تضمنت لائحة تنظيم التراخيص بالمجلس الأعلى للإعلام الصادرة بالقرار رقم 26 لسنة 2020م، والمعدلة بالقرار رقم 92 لسنة 2020م، أحكامًا تفصيلية تضبط مشروعية مزاولة هذه الأنشطة الرقمية عبر هذه المواقع، وعلى رأس هذه الشروط يأتي اشتراط أسبقية الحصول على ترخيص من المجلس الأعلى للإعلام، وكذلك في حالة التصرف في حصة منها إلى الغير أو الاندماج مع كيان آخر.

ومن الأمثلة على ذلك، ما تنص عليه المادة 31 من هذه اللائحة، حيث جاء فيها: "يجوز لشركات تقديم نقل المحتوى أن تنقل المحتوى مسجلًا أو مباشرًا من داخل جمهورية مصر العربية عبر الأقمار الصناعية أو شبكة المعلومات الدولية (الإنترنت)، ولا يجوز نقل أي مواد يخالف محتواها أحكام الدستور أو القانون أو القرارات الصادرة تنفيذًا له، أو ما يدعو إلى العنف أو يحض على التمييز أو العنصرية أو الكراهية، أو يخالف النظام العام أو الآداب العامة".

كما تنص المادة 35 من ذات اللائحة على أنه: "يجب على الشركات المرخص لها بتقديم خدمات نقل المحتوى الاحتفاظ بكافة المواد التي تم نقلها لمدة لا تقل عن سنة من تاريخ النقل، وتلتزم بإيداع نسخة منها لدى المجلس الأعلى عند طلبها. كما يجب أن توجد نسخة من الخوادم الإلكترونية التي تستضيف النسخة الإلكترونية في مكان تحدده الشركة داخل جمهورية مصر العربية، شريطة أن يكون آمنًا ومعلومًا للمجلس الأعلى، ولا يجوز تغييره إلا بعد موافقة المجلس الأعلى".

ووفقًا لما تقدم، تشكل هذه المواد إطارًا قانونيًا دقيقًا لتنظيم الأنشطة الرقمية، بما يضمن التوازن بين حرية ممارسة هذه الأنشطة وضرورة الحفاظ على النظام العام والقيم المجتمعية. كما تبرز أهمية هذه الأحكام من خلال فرض التزامات على مقدمي خدمات نقل المحتوى، تضمن توافق المواد المنقولة مع الدستور والقوانين، وتجنب نشر المحتويات التي تحض على الكراهية أو التمييز. كما تفرض اللائحة على الشركات الاحتفاظ بنسخ من المحتوى المنقول لتمكين الجهات الرقابية من مراجعتها عند الحاجة، مع اشتراط استضافة الخوادم الإلكترونية داخل البلاد لضمان السيادة الرقمية. فتعزز هذه الأحكام قدرة السلطات على مراقبة الأنشطة الرقمية ومنع الانتهاكات، بما في ذلك التنمر الإلكتروني، من خلال تطبيق ضوابط قانونية صارمة تحمي المجتمع وتضمن الالتزام بالقيم الوطنية.

ثانيًا– القرارات الفردية المستقلة:

قد تضطر الإدارة إلى ممارسة سلطتها في الضبط الإداري من خلال إصدار أوامر فردية، وهي قرارات تصدرها الإدارة بهدف تطبيقها على شخص محدد بذاته أو على مجموعة من الأشخاص محددين بذواتهم[1].

وقد تتخذ القرارات الفردية المستقلة التي تصدرها سلطات الضبط الإداري الإلكتروني في مواجهة التنمر الإلكتروني أشكالًا متعددة، وفقًا لطبيعة الحالة والهدف من التدخل؛ ففي بعض الحالات، قد تصدر أوامر تلزم المنصات الرقمية بتنفيذ إجراءات محددة، مثل اعتماد تقنيات الذكاء الاصطناعي لمراقبة التعليقات والمنشورات بشكل دقيق وتحليلها لحجب المحتوى المسيء فورًا، كما يمكن أن تتضمن هذه القرارات فرض عقوبات مالية أو اتخاذ تدابير حظر مؤقت أو دائم على الأفراد أو الكيانات التي يثبت تورطها في ممارسات التنمر الإلكتروني.

ومن جانب آخر، قد تصدر السلطات أوامر تُلزم بالامتناع عن القيام بأفعال معينة، مثل منع الترويج أو الدعم لمنصات إلكترونية تتهاون في اتخاذ خطوات فعالة لمكافحة التنمر الإلكتروني، أو تلك التي لديها سجل سابق في عدم التعامل بجدية مع شكاوى التنمر، كما قد تشمل هذه الأوامر الامتناع عن منح التراخيص اللازمة لمواقع أو تطبيقات إلكترونية لا تلتزم

---

[1] يراجع: د. محمد رفعت عبد الوهاب، مبادئ وأحكام القانون الإداري، مرجع سابق، ص 241؛ د. محمد علي حسونة، حدود سلطات الضبط الإداري وأثرها على الحريات العامة، مرجع سابق، ص 169؛ د. يوسف ناصر حمد الظفيري، الضبط الإداري وحدود سلطاته في الظروف العادية والظروف الاستثنائية، مجلة البحوث القانونية والاقتصادية، المجلد 10، العدد 74، كلية الحقوق، جامعة المنصورة، ديسمبر 2020م، ص 1516.

بالمعايير الصارمة التي تفرضها السلطات، مثل عدم وجود أنظمة مراقبة كافية أو سياسات واضحة للتعامل مع الشكاوى المتعلقة بالتنمر.

ويثور هنا تساؤل هام هو: هل يجوز لسلطات الضبط الإداري الإلكتروني أن تصدر قرارات ضبط فردية مستقلة دون أن تستند إلى قاعدة تنظيمية عامة واردة في القانون أو في لائحة تنظيمية؟

أجاب على هذا التساؤل جانب كبير من الفقه الفرنسي، حيث قرر أن قرارات الضبط الفردية التي تصدرها الإدارة يجب أن تستند إلى نص تنظيمي عام، سواء كان نصًا تشريعيًا أم نصًا لائحيًا، وذلك تحقيقًا لمبدأ المشروعية في جانبه الشكلي. ويقتضي هذا المبدأ أن تكون أوامر الضبط الفردية التي تصدرها السلطات الإدارية قائمة على أساس قانوني أو لائحي يحدد إطارها ويضفي عليها الشرعية اللازمة. وبناءً على ذلك، لا يجوز لسلطات الضبط الإداري الإلكتروني إصدار أي قرار ضبط فردي مستقل دون أن يكون له سند قانوني أو لائحي صريح، وإلا كان القرار عرضة للطعن بالبطلان لمخالفته مبدأ المشروعية[1].

ومن الناحية العملية، نجد أن هذا الموقف الفقهي يصطدم باعتبارات بالغة الأهمية، لا يمكن التهوين من تأثيرها، وهي أن اللوائح التنظيمية العامة لا يمكنها التنبؤ بجميع الوقائع أو التعامل مع كل تفصيل دقيق في الحياة الواقعية. بالإضافة إلى ذلك، هناك حالات استثنائية لا تبرر استصدار لائحة تنظيمية عامة بشأنها نظرًا لندرة وقوعها، وإذا لم تصدر لائحة أو لم تتضمن لائحة قائمة الحكم الواجب تطبيقه في حالة معينة، وحدث اضطراب خاص يتطلب التدخل، فلا ينبغي في مثل هذه الظروف أن تبقى سلطات الضبط الإداري مكتوفة الأيدي[2].

---

(1) "Toute decision administrative particutiere sur une matiere donnee doit avoir ete precedee d'une disposition generale par voie legislative ou par voie reglementaire, edictee sur la meme matiere, de facon a ce que le particulier soit soumis au general–".

–HAURIOU (M–): Precis de droit admmislratif, 12°ed, 1933, p 577.

"Les ordres et les defenses doivent toujours s'appuyer sur une disposition generale, loi ou reglement–".

– HOLLAND (L–): prscis de droit admmistratif, 9eed, 1953, p 472.

(2) يراجع: د. توفيق شحاتة، مبادئ القانون الإداري، مرجع سابق، ص 343 وما بعدها؛ د. مازن ليلو راضي، القانون الإداري، مرجع سابق، ص 62.

وقد ذهب بعض الفقه إلى أن التشريع أو اللوائح التنظيمية لا يمكن أن تستوعب جميع التوقعات أو التنبؤات المحتملة التي قد تنشأ، وبما أن الضبط الإداري يُمارس بهدف المحافظة على النظام العام أو إعادته إلى مساره الطبيعي، ونظرًا لتغير مضمون هذا المفهوم بمرور الزمن، فإنه إذا ظهر تهديد أو إخلال خاص لم يكن التشريع أو اللائحة قد توقعاه، وطلبنا في كل حالة أن يكون القرار الفردي مستندًا إلى قاعدة تنظيمية عامة، فإن ذلك يعني فعليًا تجريد سلطة الضبط من فاعليتها وقدرتها على الاستجابة الفورية والفعالة[1].

وبناءً على ما تقدم، يجب أن تتمتع سلطات الضبط الإداري الإلكتروني في مواجهة التنمر الإلكتروني بقدر كافٍ من المرونة يسمح لها باتخاذ قرارات فردية مستقلة عند الضرورة، حتى في الحالات التي لا يوجد فيها نص تنظيمي محدد يوضح الإجراء الواجب اتخاذه، فهذه المرونة ضرورية لضمان حماية النظام العام الرقمي والحفاظ على أمن وسلامة المجتمع الإلكتروني، خاصة في ظل التطور السريع للتقنيات الرقمية وظهور تهديدات جديدة لم يكن المشرع قد توقعها عند وضع القوانين واللوائح. لذلك فإن قدرة السلطات على التصرف بفعالية وسرعة في مواجهة حالات التنمر الإلكتروني هي عنصر أساسي لضمان ردع تلك الممارسات وحماية الأفراد من آثارها السلبية، دون التقيد الصارم بوجود قاعدة تنظيمية سابقة تغطي جميع الاحتمالات.

ثالثًا- التنفيذ المباشر:

يعرف التنفيذ المباشر بأنه: "حق الإدارة في تنفيذ أوامرها على الأفراد بالقوة الجبرية إذا امتنعوا عن تنفيذها طواعية، دون الحاجة إلى إذن مسبق من القضاء"[2]. ويُعد هذا الحق من

---

[1] "Le reglement ou la loii on le salt, ne peuvent tout prevoir- Or la police est une activite qui s'exerce en vue du maintien ou du retablissement de l'ordre public et on a vu que le contenu de cette derniere notion est loin d'etre immuable- Si bien qu'un trouble, un desordre particulier, peuvent fort bien apparaitre alors qu'ils n'ont pas ete prevus par le legislateur ou par l'autorice reglementaire- Admettre que toute mesure mdividuelle de police suppose un acte-regle preetabli/ c'est nsquer de laisser souvent l'autorite de police desarmee".

- CASTAGNE (J.) Le controle juridictonnel de la legalite des actes de police administrative "th, paris, 1961, Bordeaux, ed 1964, p 40.

[2] د. سليمان محمد الطماوي، النظرية العامة للقرارات الإدارية، مرجع سابق، ص 573؛ د. محمود سعد الدين الشريف، أساليب الضبط الإداري والقيود الواردة عليه، مجلة مجلس الدولة المصري، السنة الثانية عشرة، 1964م، ص 44.

أبرز الامتيازات التي تتمتع بها الإدارة، إذ يُمكّنها من التدخل الفوري لمنع الإخلال بالنظام العام أو لإعادة النظام إلى حالته الطبيعية دون الحاجة إلى الحصول على إذن قضائي مسبق.

وبمقتضى هذا الحق، تستطيع الإدارة، في حالة امتناع الأفراد عن تنفيذ قراراتها طوعًا، أن تستوفي حقوقها بالقوة إذا اقتضى الأمر ذلك. والأصل أن تلجأ الإدارة، كغيرها من الأفراد، إلى القضاء للحصول على حقوقها، إلا أن إجراءات التقاضي قد تستغرق وقتًا طويلًا، مما قد يعيق الإدارة عن تحقيق المصلحة العامة التي تتطلب أحيانًا تنفيذًا سريعًا لقراراتها. ولذلك منحها القانون الحق في التنفيذ الجبري في حالات معينة تحقيقًا للصالح العام[1].

ويُعتبر التنفيذ الجبري المباشر أسلوبًا استثنائيًا يُمنح للإدارة، حيث يحرم الأفراد من ضمانات اللجوء إلى القضاء، ويسمح لهيئات الضبط الإداري باتخاذ إجراءات صارمة، قد تتسم بالشدة في كثير من الأحيان. وعلى الرغم من المخاطر المرتبطة بهذا الأسلوب، فإن الاعتبارات العملية في مجال التصرف الإداري عمومًا تبرره، إلا أنه يصبح أكثر ضرورة في مجال الضبط الإداري الإلكتروني، الذي يهدف إلى المحافظة على النظام العام الرقمي، فيتطلب هذا الهدف في بعض الأحيان اتخاذ إجراءات سريعة وحاسمة لا تحتمل التأخير، وقد تُفقد فاعليتها إذا أخضعت لضرورة الحصول على إذن قضائي مسبق.

ولا يُفهم من حق التنفيذ الجبري المباشر الممنوح لسلطات الضبط الإداري الإلكتروني في مواجهة التنمر الإلكتروني، أنه يتيح للإدارة الاستيلاء على ما ليس لها أو الاعتداء على حقوق الأفراد أو ممتلكاتهم بغير حق، أو انتهاك القانون بشكل تعسفي دون رادع أو جزاء، بل إن هذا الحق مقيد بضوابط مشروعية صارمة، تُلزم الإدارة بعدم تجاوز حدود الضرورة أو التعدي على حقوق الأفراد بشكل غير مبرر، ويظل للأفراد الحق الكامل في اللجوء إلى القضاء لرد أي اعتداء غير مشروع يقع عليهم من جانب السلطات الإدارية.

ونظرًا لأهمية الضرورة وما يترتب عليها من آثار خطيرة، فقد حدد الفقه شروطًا صارمة لتطبيقها، وأكد القضاء على ضرورة الالتزام بهذه الشروط، وفي إطار التنفيذ المباشر الذي تتخذه

---

[1] د. مهند قاسم زغير، السلطة التقديرية في مجال الضبط الإداري في الظروف العادية، مرجع سابق، ص 136.

سلطات الضبط الإداري الإلكتروني لمواجهة التنمر الإلكتروني، يجب توافر الشروط التالية لضمان مشروعية هذا التنفيذ[1]:

1- **مشروعية القرار**: يجب أن يكون التنفيذ الجبري مستندًا إلى قرار مشروع، سواء كان ذلك القرار تطبيقًا لنص تشريعي أم لائحي، ولا يشترط أن يكون قرار الضبط الفردي مكتوبًا أو منشورًا؛ إذ يمكن أن يكون القرار شفويًا طالما كان مستندًا إلى أساس قانوني صحيح.
2- **وجود مقاومة للتنفيذ**: يشترط أن تواجه الإدارة مقاومة من الجهة المعنية بتنفيذ قرار الضبط، مما يستتبع على جهة الضبط توجيه أمر واضح لصاحب الشأن بضرورة التنفيذ، مع منحه مهلة معقولة للامتثال قبل اللجوء إلى استخدام القوة الجبرية.
3- **التناسب في استخدام القوة**: يجب أن يقتصر استخدام القوة الجبرية على ما هو ضروري لتفادي الخطر الوشيك الناجم عن عدم تنفيذ قرار الضبط، ويجب أن تكون الإجراءات المتخذة متناسبة مع درجة الخطر. ويراقب القاضي الإداري تحقق هذه الشروط لضمان أن التنفيذ الجبري لا يتجاوز ما تقتضيه الضرورة.

وبتطبيق هذه الشروط، تضمن سلطات الضبط الإداري الإلكتروني أن يكون تنفيذها الجبري المباشر لمواجهة التنمر الإلكتروني مشروعًا، ومراعيًا لحقوق الأفراد ومصالحهم، بما يتناسب مع خطورة الموقف ومتطلبات الحفاظ على النظام العام الرقمي.

وهديًا على ما تقدم، وضع الفقه والقضاء في فرنسا ومصر شروطًا صارمة لضمان مشروعية هذا التنفيذ؛ فيشكل شرط مشروعية القرار حجر الزاوية في هذا الإطار، إذ يُشترط أن يستند التنفيذ الجبري إلى قرار قانوني واضح، سواء كان تشريعيًا أم لائحيًا، مما يضمن أن يكون الإجراء مدعومًا بسلطة قانونية صحيحة، حتى لو كان القرار شفويًا، ويُعد شرط وجود مقاومة للتنفيذ ضروريًا لضمان احترام حقوق الأفراد، حيث يُلزم الإدارة بإعطاء المهلة الكافية لصاحب الشأن للامتثال قبل استخدام القوة، مما يعكس التزام الإدارة بمبادئ العدالة والإنصاف، أما شرط التناسب في استخدام القوة، فيُظهر حرص الفقه والقضاء على ألا يتجاوز التنفيذ الجبري حدود الضرورة، وأن يكون استخدام القوة مقيدًا بما يتطلبه الخطر الوشيك فقط، لضمان عدم إساءة

---

[1] لمزيد من التفصيل حول هذه الشروط يراجع: د. فيصل كامل إسماعيل، سلطات الضبط الإداري أثناء حالة الطوارئ في مصر وفرنسا والولايات المتحدة الأمريكية، رسالة دكتوراة، كلية الحقوق، جامعة المنصورة، 2006م، ص 376 وما بعدها؛ د. محمد علي حسونة، حدود سلطات الضبط الإداري وأثرها على الحريات العامة، مرجع سابق، ص 173-174.

- CASTAGNE (J-): op- cst- I ,pp 45-46.

استعمال السلطة. وتشكل هذه الشروط مجتمعة ضمانة قانونية للحفاظ على شرعية وفعالية التدخلات الإدارية في مواجهة التحديات الرقمية المستجدة، مثل التنمر الإلكتروني، مع الحفاظ على حقوق الأفراد في إطار المصلحة العامة.

ومثالًا على تطبيق السلطات التنظيمية للتنفيذ المباشر في مواجهة التنمر الإلكتروني، ما تنص عليه المادة 55 من قانون تنظيم الاتصالات، التي تمنح الجهاز القومي لتنظيم الاتصالات الصلاحية في استخدام الوسائل التي تُمكنه من الكشف عن استخدامات الترددات غير المرخص بها، والتحقق من التزام المرخص لهم بشروط الترخيص. كما يخوّل للجهاز حق التفتيش على الأجهزة اللاسلكية المصرح بها للتحقق من مطابقتها لشروط الترخيص، وذلك بالتنسيق مع القوات المسلحة وأجهزة الأمن القومي، لضمان عدم المساس بالأنظمة المعمول بها لديها.

ويُلاحظ أن لفظة "الوسائل" الواردة في هذا النص جاءت عامة، دون تخصيص أو تقييد، مما يعني أنها تشمل كافة الوسائل التي تُمكن الجهاز من تنفيذ التزاماته المنصوص عليها، سواء كانت قانونية أم مادية، بما في ذلك استخدام القوة الجبرية إذا اقتضت الضرورة[1]. وينطبق هذا المبدأ على هيئات الضبط الإداري الإلكتروني في مواجهة التنمر الإلكتروني؛ حيث تملك هذه الهيئات صلاحية اتخاذ كافة الإجراءات اللازمة لضمان الامتثال للقوانين واللوائح، بما في ذلك التدخل الفوري واستخدام القوة الجبرية عند الضرورة لحماية النظام العام الرقمي، وضمان التزام الجهات المرخصة بشروط ترخيصها وعدم الإخلال بها.

رابعًا- الجزاء الإداري الوقائي:

يعرف الجزاء الإداري الوقائي بأنه: إجراء وقائي تتخذه الإدارة كوسيلة استباقية تهدف إلى درء خطر الإخلال بالنظام العام، وذلك من خلال منع مصدر التهديد من الفرصة أو القدرة على إحداث الضرر المحتمل[2].

وبذلك، يعد الجزاء الإداري الوقائي من أهم الأدوات التي تملكها سلطات الضبط الإداري الإلكتروني في مواجهة التنمر الإلكتروني؛ حيث يُستخدم للضغط على إرادة المخالفين وإلزامهم بالامتثال للقانون، وتضمنت لوائح الضبط الإداري في هذا الإطار جزاءات وقائية تُوقع على

---

[1] د. حسين مقداد عبد اللطيف، دور الضبط الإداري في الحد من مخاطر الفضاء الإلكتروني في مصر وفرنسا، مرجع سابق، ص 743-744.

[2] د. صلاح يوسف عبد العليم، أثر القضاء الإداري على النشاط الإداري للدولة، دار الفكر العربي، الإسكندرية، 2008م، ص 30.

الأفراد أو الجهات التي تتوافر بشأنها شروط توقيع هذه الجزاءات، بهدف ردعهم عن الانخراط في أي نشاط رقمي يتسبب في تهديد النظام العام الرقمي، سواء كان ذلك بالتحريض على التنمر الإلكتروني أم المشاركة فيه.

كما تهدف هذه الجزاءات إلى منع تكرار مثل هذه الأفعال مستقبلًا، خصوصًا إذا كان المخالفون يرغبون في العودة إلى ممارسة أنشطتهم الرقمية مرة أخرى. ومن هنا تأتي تسمية هذه الجزاءات بـ"الجزاءات الوقائية"، حيث تلعب دورًا محوريًا في حماية الفضاء الإلكتروني وضمان الالتزام بالقواعد التي تحافظ على أمن وسلامة المجتمع الرقمي.

ومن الأمثلة العملية على ممارسة هذه الصلاحية الجوهرية لسلطات الضبط الإداري الإلكتروني، ما نص عليه قرار وزير الاتصالات وتكنولوجيا المعلومات رقم 464 لسنة 2015 بإصدار لائحة الجزاءات التي يوقعها الجهاز القومي لتنظيم الاتصالات على الجهات المرخص لها بالعمل في مجال الاتصالات[1]، حيث تنص المادة 17 منها على أنه: "مع عدم الإخلال بالعقوبات الجنائية المنصوص عليها في قانون الاتصالات أو في أي قانون آخر، يُجازى المخالف بالجزاءات المنصوص عليها في هذه اللائحة والمحددة في الجدول المرفق بها". ومثال آخر هو قرار رئيس المجلس الأعلى لتنظيم الإعلام رقم 16 لسنة 2019 بشأن إصدار لائحة الجزاءات والتدابير التي يجوز توقيعها على الجهات الخاضعة لأحكام قانون تنظيم الإعلام والمجلس الأعلى لتنظيم الإعلام الصادر بالقانون رقم 180 لسنة 2018[2].

وتنقسم الجزاءات الإدارية الوقائية إلى نوعين رئيسيين: الجزاءات المالية والجزاءات غير المالية، وذلك على النحو الآتي:

1- الجزاءات المالية:

ومثال هذه الجزاءات في فرنسا، تنص المادة 83 من اللائحة العامة لحماية البيانات الأوروبية، الصادرة بقرار المجلس الأوروبي رقم 679 لسنة 2016م، المتعلقة بحماية الأفراد في ما يخص معالجة البيانات الشخصية وحرية نقلها، على أنه: "يتعين على كل سلطة إشرافية أن تضمن أن الغرامات الإدارية المفروضة بموجب هذه المادة فيما يتعلق بالانتهاكات المذكورة في الفقرات 4 و5 و6 منها تكون فعالة، ومتناسبة، ورادعة. وبناءً على الظروف المحيطة بكل حالة

---

[1] الوقائع المصرية، العدد 121 (تابع)، السنة 188هـ، الأربعاء 9 شعبان 1436هـ، الموافق 27 مايو 2015م.

[2] الوقائع المصرية، العدد 64، الصادر في 18 مارس 2019م.

على حدة، تُفرض غرامات إدارية، ... وعند اتخاذ قرار بفرض غرامة إدارية، يجب أخذ الاعتبارات الواردة في البنود من (أ) إلى (ك) من هذه الفقرة".

وفي حال ارتكبت وحدة تحكم أو معالج، عن عمد أو بإهمال، عدة انتهاكات لأحكام هذه اللائحة، ضمن نفس عملية المعالجة أو العمليات ذات الصلة، فلا يجوز أن يتجاوز إجمالي الغرامة الإدارية المبلغ المحدد للانتهاك الأشد خطورة. وتخضع المخالفات المتعلقة بـ: (أ) التزامات وحدة التحكم والمعالج بموجب المواد 8 و11 و25 إلى 39 و42 و43؛ (ب) التزامات هيئة إصدار الشهادات بموجب المادتين 42 و43؛ (ج) التزامات الهيئة المسؤولة عن مراقبة مدونات السلوك بموجب المادة 41، لغرامات إدارية تصل إلى 10,000,000 يورو، أو ما يصل إلى 2% من إجمالي المبيعات السنوية للسنة المالية السابقة بالنسبة للشركات، أيهما أكبر.

وتخضع الانتهاكات التالية لعقوبات مالية صارمة: (أ) انتهاك المبادئ الأساسية لمعالجة البيانات، بما في ذلك الشروط المتعلقة بالحصول على الموافقة وفقًا للمواد 5 و6 و7 و9؛ (ب) المساس بالحقوق الممنوحة لأصحاب البيانات بموجب المواد من 12 إلى 22؛ (ج) نقل البيانات الشخصية إلى جهة مستلمة في دولة ثالثة أو إلى منظمة دولية وفقًا للمواد من 44 إلى 49؛ (د) أي التزامات ناشئة عن التشريعات الوطنية للدول الأعضاء التي تم تبنيها بموجب الفصل التاسع؛ (هـ) عدم الامتثال لأمر قضائي أو قرار مؤقت أو دائم يحد من معالجة البيانات أو يعلق تدفقها، كما تأمر به السلطة الإشرافية وفقًا للمادة 2/58، أو الإخفاق في منح الوصول المطلوب، بما يمثل انتهاكًا للمادة 1/58.

وتخضع هذه الانتهاكات لغرامات إدارية تصل إلى 20,000,000 يورو أو ما يصل إلى 4% من إجمالي الإيرادات السنوية العالمية للسنة المالية السابقة للشركة، أيهما أكبر. وفي حال عدم الامتثال لأمر صادر عن السلطة الإشرافية وفقًا للمادة 2/58، فإن العقوبات المالية قد تصل إلى المبلغ المذكور أو نسبة 4% من إجمالي حجم التداول السنوي العالمي للسنة المالية السابقة، أيهما أكبر.

وإذا لم ينص النظام القانوني لدولة عضو على فرض الغرامات الإدارية، يمكن تطبيق هذه المادة بحيث يتم تحديد الغرامة من قبل السلطة الرقابية المختصة وفرضها من قبل المحاكم الوطنية المختصة، مع التأكد من أن هذه الوسائل القانونية فعّالة ولها تأثير مكافئ للغرامات الإدارية التي تفرضها السلطات الرقابية. وفي جميع الأحوال، تكون الغرامات المفروضة فعّالة، ومتناسبة، ورادعة. وتقوم الدول الأعضاء المعنية بإخطار المفوضية الأوروبية بالأحكام القانونية

التي تعتمدها بموجب هذه الفقرة في موعد أقصاه 25 مايو 218، وبأي أحكام قانونية تعديلية لاحقة أو أي تعديلات أخرى ذات صلة دون تأخير.

ومن أمثلة هذه الجزاءات في مصر، ما ورد في المادة 18 من لائحة الجزاءات التي يوقعها الجهاز القومي لتنظيم الاتصالات، من أنه: "يجوز في حالة ارتكاب المخالف مخالفة غير منصوص عليها في الجدول المرفق بهذه اللائحة، أن يتم توقيع الجزاءات التالية عليه: (أ) الخصم من مبلغ تأمين الترخيص أو التصريح؛ (ب) ...؛ (ج) إلزام المخالف بإزالة أسباب المخالفة على نفقته الخاصة؛ (د) حرمان المخالف من ... أو من تعديل التعريفة لفترة محددة".

كما اشتملت لائحة الجزاءات والتدابير التي يجوز توقيعها على الجهات الخاضعة لأحكام قانون تنظيم الصحافة والإعلام والمجلس الأعلى لتنظيم الإعلام، الصادرة بقرار رئيس المجلس الأعلى لتنظيم الإعلام رقم 16 لسنة 2019، على العديد من الجزاءات المالية. فمثلًا تنص المادة 18 على أنه: "تناول الوسيلة الإعلامية أو الصحيفة أو الموقع الإلكتروني لسلوك المشتغل بالعمل العام أو الشخص ذي الصفة النيابية أو المكلف بخدمة عامة فيما يخص مسألة وثيقة الصلة بعمله بهدف تحقيق المصلحة العامة، وإلا عُدَّ هذا التناول مخالفًا، ويستلزم توقيع أحد الجزاءات التالية أو بعضها حسب ما يراه المجلس الأعلى للإعلام مناسبًا: 1. ... 3. أداء مبلغ مالي لا يزيد عن مائة ألف جنيه مصري أو ما يعادلها بالعملة الأجنبية".

وبالمثل، تنص المادة 19 من اللائحة ذاتها على أنه: "يعد قيام الصحيفة أو الوسيلة الإعلامية أو الموقع الإلكتروني بنشر أو بث مادة صحفية أو إعلامية أو إعلانية تحتوي على ظهور أطفال أثناء التحقيق معهم أو محاكمتهم جنائيًا، يعتبر مخالفة تستوجب توقيع أحد الجزاءات التالية أو بعضها حسب تقدير المجلس الأعلى لتنظيم الإعلام: 1. ..؛ 3. أداء مبلغ مالي لا يزيد عن مائتي ألف جنيه مصري أو ما يعادلها بالعملة الأجنبية".

وبناءً على ما تقدم، تتمثل سلطات الضبط الإداري الإلكتروني في النظامين الفرنسي والمصري في قدرة السلطات الرقابية على فرض جزاءات فعّالة ورادعة لمواجهة الانتهاكات المتعلقة بحماية البيانات الشخصية والتصرفات غير القانونية في الفضاء الإلكتروني، بما في ذلك التنمر الإلكتروني. في فرنسا، تُلزم المادة 83 من اللائحة العامة لحماية البيانات الأوروبية (GDPR) السلطات الإشرافية بضمان أن تكون الغرامات الإدارية المفروضة متناسبة وفعالة بما يكفل الردع، حيث يمكن أن تصل هذه الغرامات إلى 20 مليون يورو أو 4% من الإيرادات السنوية العالمية للشركة، أيهما أكبر، لضمان الالتزام بالقوانين والمعايير المتعلقة بحماية البيانات. وفي مصر، يمارس الجهاز القومي لتنظيم الاتصالات والمجلس الأعلى لتنظيم الإعلام

سلطاتهما من خلال فرض جزاءات مالية وغير مالية، تتضمن إلزام المخالفين بإزالة أسباب المخالفة على نفقتهم، وحرمانهم من تسويق الخدمات أو تعديل التعريفة لفترات محددة، بالإضافة إلى فرض غرامات مالية على الوسائل الإعلامية التي تتناول سلوك الشخصيات العامة بشكل غير مبرر أو تنشر مواد تحتوي على ظهور أطفال أثناء التحقيق معهم. فتسهم هذه التدابير الوقائية في حماية المجتمع من التنمر الإلكتروني وغيره من أشكال الإساءة في البيئة الرقمية.

2- الجزاءات غير المالية:

تنص المادة 84 من اللائحة العامة لحماية البيانات الأوروبية على أنه: "تتولى الدول الأعضاء تحديد قواعد العقوبات الأخرى المطبقة في حالة انتهاك أحكام هذه اللائحة، لا سيما تلك الانتهاكات التي لا تخضع للغرامات الإدارية المنصوص عليها في المادة 83. ويجب على الدول الأعضاء اتخاذ جميع التدابير اللازمة لضمان أن تكون هذه العقوبات فعالة، ومتناسبة، ورادعة. كما يجب على كل دولة عضو إخطار المفوضية الأوروبية بالأحكام القانونية التي تعتمدها بموجب هذه المادة بحلول 25 مايو 2018 كحد أقصى، وإخطارها بأي تعديل لاحق يؤثر على تلك الأحكام دون تأخير".

وفي مصر، تضمنت لائحة الجزاءات التي يوقعها الجهاز القومي لتنظيم الاتصالات على الجهات المرخص لها بالعمل في مجال الاتصالات العديد من الجزاءات غير المالية، التي يمكن إدراجها ضمن مفهوم الجزاءات الوقائية التي تمارسها سلطة الضبط الإداري الإلكتروني. على سبيل المثال، تنص المادة 18 من اللائحة المذكورة على أنه: يجوز في حالة ارتكاب المخالف مخالفة أخرى غير المنصوص عليها في الجدول المرفق، توقيع الجزاءات التالية عليه: (أ) ...؛ (ب) حرمان المخالف من تسويق الخدمة المرخص بها أو الأجهزة والمعدات المصرح له بها لفترة محددة؛ (ج) إلزام المخالف بإزالة أسباب المخالفة في مدة محددة؛ (د) حرمان المخالف من تقديم العروض الترويجية أو من تغيير التعريفة لفترة محددة".

كما تضمنت لائحة الجزاءات والتدابير التي يجوز توقيعها على الجهات الخاضعة لأحكام قانون تنظيم الصحافة والإعلام والمجلس الأعلى لتنظيم الإعلام، جزاءات أخرى تتعلق بسلوك وسائل الإعلام، فتنص المادة 18 من اللائحة على أنه: "إذا تناولت الوسيلة الإعلامية أو الصحيفة أو الموقع الإلكتروني مسلك المشتغل بالعمل العام أو الشخص ذي الصفة النيابية أو المكلف بخدمة عامة بطريقة لا تخدم المصلحة العامة، يُعتبر هذا التناول مخالفة تستوجب توقيع أحد الجزاءات التالية أو بعضها وفقًا لتقدير المجلس الأعلى لتنظيم الإعلام: 1. لفت النظر؛ 2. إلزام الوسيلة بتقديم اعتذار بذات الطريقة التي ارتكبت بها المخالفة ...".

وبالمثل، تنص المادة 19 من ذات اللائحة على أنه: "في حال قيام الصحيفة أو الوسيلة الإعلامية أو الموقع الإلكتروني ببث أو نشر مادة صحفية أو إعلامية أو إعلانية تتضمن وجود أطفال أثناء التحقيق معهم أو محاكمتهم جنائيًا، يُعد ذلك مخالفة تستوجب توقيع أحد الجزاءات التالية أو بعضها حسب تقدير المجلس الأعلى لتنظيم الإعلام: 1. لفت النظر؛ 2. إلزام الوسيلة بتقديم اعتذار بذات الطريقة التي ارتكبت بها المخالفة ...".

وهديًا على ما تقدم، تتجلى سلطات الضبط الإداري الإلكتروني في مواجهة التنمر الإلكتروني، في كل من النظامين الفرنسي والمصري من خلال مجموعة من العقوبات الرادعة والفعالة التي تهدف إلى حماية الأفراد من الاعتداءات الرقمية. ففي فرنسا، تنص المادة 84 من اللائحة العامة لحماية البيانات الأوروبية على أن الدول الأعضاء تلتزم بتحديد قواعد العقوبات الأخرى غير المالية، التي تُفرض في حالة انتهاك أحكام اللائحة، مع ضرورة اتخاذ جميع التدابير اللازمة لضمان أن تكون هذه العقوبات متناسبة ورادعة وفعالة، بما في ذلك إبلاغ المفوضية الأوروبية بأي أحكام قانونية جديدة أو تعديلات لاحقة. أما في مصر، فقد تضمنت لائحة الجزاءات التي يصدرها الجهاز القومي لتنظيم الاتصالات، وكذلك المجلس الأعلى لتنظيم الإعلام، إجراءات صارمة تشمل حرمان المخالفين من تسويق خدماتهم أو تعديل تعريفتهم لفترة محددة، وإلزامهم بإزالة أسباب المخالفة على نفقتهم الخاصة. كما يُفرض على الوسائل الإعلامية التي تتناول سلوك الشخصيات العامة بطريقة غير مبررة أو تنشر محتوى يضر بالأطفال أثناء التحقيق معهم عقوبات تتراوح بين لفت النظر وتقديم الاعتذارات العلنية.

المطلب الثالث

إجراءات الضبط الإداري الإلكتروني لمواجهة التنمر الإلكتروني

تمهيد وتقسيم:

تتولى هيئات الضبط الإداري الإلكتروني المختصة بمكافحة التنمر الإلكتروني اتخاذ مجموعة من الإجراءات المتنوعة التي تهدف إلى مكافحة هذا النوع من الجرائم الإلكترونية. وتختلف هذه الإجراءات تبعًا لطبيعة التدخل المطلوب؛ فبعضها يتسم بالطابع الوقائي، حيث يتم اتخاذه قبل أن يباشر الأفراد نشاطًا معينًا، وذلك بهدف الحيلولة دون وقوع التنمر الإلكتروني. بينما تتسم الإجراءات الأخرى بالطابع العلاجي، حيث تهدف إلى معالجة الأفعال التي قد تصنف ضمن جرائم التنمر الإلكتروني بعد وقوعها.

ولكن تواجه هيئات الضبط الإداري تحدياتٍ عميقة في مكافحة التنمر الإلكتروني؛ حيث تتداخل الطبيعة العابرة للحدود لهذا النوع من الجرائم مع تعقيدات التقنيات الحديثة وتطور أساليب الجناة في إخفاء هوياتهم ومواقعهم. إن التحديات التقنية والقانونية التي تفرضها الوسائط الرقمية، من غياب النصوص القانونية الواضحة التي تتعامل بشكل مباشر مع هذا السلوك، إلى صعوبة تتبع وتوثيق الأدلة الرقمية بما يتوافق مع معايير الإثبات القانونية، تضع هيئات الضبط أمام مهمة شاقة لتحقيق الردع وحماية الأفراد من الآثار النفسية والاجتماعية لهذه الجرائم المستترة.

وبناءً على ما تقدم، يقسم هذا المطلب إلى ثلاثة أفرع على النحو الآتي:

- **الفرع الأول:** التدابير الوقائية لهيئات الضبط الإداري لمكافحة التنمر الإلكتروني.
- **الفرع الثاني:** التدابير العلاجية لهيئات الضبط الإداري لمكافحة التنمر الإلكتروني.
- **الفرع الثالث:** الصعوبات التي تواجه هيئات الضبط الإداري الإلكتروني في مواجهة التنمر الإلكتروني وكيفية التغلب عليها.

الفرع الأول

التدابير الوقائية لهيئات الضبط الإداري لمكافحة التنمر الإلكتروني

الأصل في طبيعة الضبط الإداري– ولا سيما في مجال الضبط الإداري الإلكتروني، أنه ذو طابع وقائي بالأساس؛ إذ يسعى إلى منع وقوع الأنشطة التي قد تؤدي إلى ارتكاب مخالفات أو أفعال تصنف ضمن الجرائم المعلوماتية. ولهذا الغرض، تبادر هيئات الضبط الإداري المختصة باتخاذ إجراءات وقائية متعددة، تتنوع وفقًا لطبيعة النشاط الذي يمارسه الأفراد. ونظرًا لخصوصية الجرائم المعلوماتية، ولأن وظيفة الضبط الإداري تتمثل أساسًا في الوقاية والردع قبل وقوع الجريمة، فإن التركيز يجب أن ينصب على تلك الإجراءات الوقائية التي تتعلق بشكل مباشر بمواجهة التنمر الإلكتروني. ومن أهم التدابير أو الإجراءات الوقائية التي تتخذها هيئات الضبط الإداري الإلكتروني للحد من ظاهر التنمر الإلكتروني ما يأتي:

أولًا: الحرمان من حق استخدام الإنترنت

يقصد بتطبيق تدبير حرمان المتهم من استخدام الإنترنت كتدبير وقائي متناسب مع الجريمة المرتكبة، وهي جريمة التنمر الإلكتروني، تطبيقاً لمبدأ تناسب العقوبة مع خطورة الفعل المرتكب. ويُعد هذا التدبير إجراءً احترازيًا ضروريًا يهدف إلى منع المتهم من استغلال الوسائل الإلكترونية في ارتكاب المزيد من الجرائم، ويشابه في طبيعته سحب رخصة القيادة من شخص يقود مركبته

تحت تأثير الكحول ويتسبب في دهس أحد المارة، أو منع شخص مدان بجريمة خطرة من حيازة سلاح ناري كإجراء وقائي يهدف إلى الحيلولة دون تكرار الجريمة[1].

ويُمثل هذا التدبير أداة فعالة لهيئات الضبط الإداري الإلكتروني في ردع الأفراد عن ارتكاب جرائم التنمر الإلكتروني؛ إذ يُسهم في تعزيز الحماية الرقمية والنظام العام من خلال تقييد وصول الجناة المحتملين إلى الوسائل التي قد تُستخدم في إلحاق الأذى بالآخرين.

ثانيًا: التوعية المجتمعية

يتعين على هيئات الضبط الإداري الإلكتروني تنفيذ حملات توعوية شاملة تهدف إلى تثقيف المجتمع بمخاطر هذه الظاهرة وكيفية الوقاية منها، وتشمل هذه الحملات التعاون الوثيق مع المؤسسات التعليمية لنشر الوعي بين الطلاب وأولياء الأمور، فضلًا عن تنظيم ورش عمل ودورات تدريبية تسلط الضوء على الآثار السلبية للتنمر الإلكتروني وأهمية التصدي له.

بالإضافة إلى ذلك، ينبغي على هيئات الضبط الإداري الإلكتروني العمل على تعزيز ثقافة الاحترام والتسامح في الفضاء الرقمي من خلال مبادرات تروج للسلوكيات الإيجابية عبر الإنترنت، ما يُسهم في بناء مجتمع رقمي واعٍ ومسؤول، قادر على التعامل مع تحديات العصر الرقمي بروح من المسؤولية والاحترام المتبادل.

ثالثًا: إخفاء أو حظر التغريدات أو التعليقات المسيئة

وفي إطار تعزيز دور هيئات الضبط الإداري الإلكتروني في مكافحة التنمر الإلكتروني، يمكن اعتماد خاصية إخفاء أو حظر التغريدات أو التعليقات المسيئة على منصات التواصل الاجتماعي. فتتيح هذه الخاصية للمستخدمين حجب المحتوى غير المرغوب فيه استنادًا إلى كلمات أو عبارات معينة أو حتى محتوى المحادثات، مما يوفر حماية فعالة لأي مستخدم يتعرض لانتهاكات أو تنمر إلكتروني. وعلى سبيل المثال، قامت شركة تويتر بتعديل سياستها لحظر التهديدات بالعنف، سواء كانت مباشرة أم غير مباشرة، مع تحسين سرعة الاستجابة للبلاغات المتعلقة بسوء استخدام المنصة، مما يسهل الإبلاغ الفوري عن أي محتوى يشكل نوعًا من التنمر الإلكتروني[2].

---

[1] يراجع: د. ياسر محمد اللمعي، المواجهة الجنائية لظاهرة التنمر الإلكتروني في ضوء السياسة التشريعية الحديثة، مرجع سابق، ص 136.

[2] د. أحمد محمد عبد الباقي، التكنولوجيا وجرائم المستقبل، الطبعة الأولى، دار النهضة العربية، القاهرة، 2017م، ص 114.

وبالمثل، أطلقت شركة فيسبوك في نوفمبر 2018 ميزة تسمح للمستخدمين بإيقاف ظهور كلمات أو عبارات أو رموز تعبيرية معينة في التعليقات على شريط الأحداث الخاص بهم، دون حذفها فعليًا، حيث تظل مرئية للآخرين ولكنها لا تظهر للمستخدم على صفحته الخاصة[1].

وتطبيقًا لهذه السياسات، ألزمت محكمة الدرجة الأولى في باريس شركة فيسبوك، بصفتها مستضيفًا للبيانات، بإزالة المحتوى التحريضي على الكراهية والعنف وتقديم البيانات التي تكشف عن هوية منشئ المحتوى المخالف[2]. وبالمثل، قضت محكمة الدرجة الأولى في تولوز بمسؤولية منصات التواصل الاجتماعي عن عدم سحب المحتوى الضار وغير المشروع خلال مدة 24 ساعة من تاريخ الإبلاغ عنه، مما يؤكد ضرورة اتخاذ تدابير سريعة وفعالة لحماية المستخدمين من الأضرار الناجمة عن المحتوى الإلكتروني غير المشروع[3].

رابعًا: التعاون مع منصات الإنترنت

في إطار تعزيز فعالية هيئات الضبط الإداري الإلكتروني في مواجهة التنمر الإلكتروني، تلتزم هذه الهيئات بالتنسيق الوثيق مع منصات التواصل الاجتماعي لضمان الامتثال الكامل للتشريعات الوطنية ذات الصلة، واتخاذ التدابير الكفيلة بالحد من ظاهرة التنمر الإلكتروني. ويشمل هذا التنسيق تطوير وتنفيذ أدوات تقنية متقدمة تسهم في الإبلاغ الفوري عن حالات التنمر، والاستجابة السريعة لها، بما في ذلك إغلاق الحسابات الإلكترونية التي يثبت تورطها في هذه الممارسات، وذلك بهدف حماية الأمن السيبراني وضمان بيئة إلكترونية آمنة ومستقرة.

فيُعدّ إغلاق الحساب الإلكتروني على منصات التواصل الاجتماعي، مثل تويتر أو فيسبوك أو إنستجرام أو غيرها، تدبيرًا احترازيًا فعّالًا يُتّخذ في حال استخدام الحساب للتحريض على الكراهية أو العنف أو التمييز العنصري، أو في حال ارتكاب أفعال التحرش الإلكتروني، أو التهديد، أو الابتزاز الإلكتروني. ويُعتبر هذا التدبير إحدى الوسائل القانونية الأساسية التي

---

[1] د. ياسر محمد اللمعي، المواجهة الجنائية لظاهرة التنمر الإلكتروني في ضوء السياسة التشريعية الحديثة، مرجع سابق، ص 138-139.

[2] TGI Paris, Ordonnance de référé, 13 avril 2010, Facebook/Hervé G., www.legalis.net.

[3] TGI Toulouse, 13 Mars 2008, Krim k c/Pierre G. www.legalis.net.

تعتمدها السلطات المختصة للحد من انتشار هذه الظاهرة الإجرامية الخطيرة والحفاظ على بيئة إلكترونية آمنة[1].

خامسًا: التشجيع على استخدام التكنولوجيا الآمنة

في سياق تعزيز قدرات هيئات الضبط الإداري الإلكتروني على مواجهة التنمر الإلكتروني، يتم التركيز على تشجيع المستخدمين على تبني واستخدام تقنيات وبرامج حماية متقدمة تُمكّنهم من تحصين أنفسهم ضد التهديدات الإلكترونية، وتشمل هذه التدابير التوجيه نحو استخدام برامج الحماية السيبرانية المتطورة وضبط إعدادات الخصوصية بشكل يضمن تقليل مخاطر التعرض للتنمر الإلكتروني، وذلك في إطار استراتيجية شاملة تستهدف الوقاية والحد من هذه الظاهرة عبر تمكين الأفراد من أدوات دفاعية فعّالة ومواكبة للتطور التكنولوجي.

سادسًا: إجراء الأبحاث والدراسات العلمية المتخصصة

من أبرز الأساليب الوقائية التي تعتمدها هيئات الضبط الإداري الإلكتروني في مواجهة التنمر الإلكتروني، إجراء الأبحاث والدراسات العلمية المتخصصة، بالإضافة إلى تحليل البيانات بشكل منهجي، فيهدف هذا النهج إلى استقصاء العوامل المؤدية إلى التنمر الإلكتروني، ورصد الأنماط السلوكية التي قد تساهم في وقوع هذه الجريمة. ومن خلال هذه الأبحاث، يمكن لهيئات الضبط الإداري تطوير استراتيجيات استباقية فعّالة تهدف إلى منع حدوث التنمر الإلكتروني قبل وقوعه، عبر توجيه الجهود نحو الفئات الأكثر عرضة للخطر، وتوعية المجتمع بمخاطر هذه الظاهرة، وصياغة سياسات وقائية تستند إلى أسس علمية متينة. ومن ثم، تُعد هذه الأدوات البحثية حجر الزاوية في تعزيز قدرة الهيئات على التصدي لظاهرة التنمر الإلكتروني بفعالية وشمولية.

سابعًا: تنفيذ برامج مراقبة متقدمة

يعتبر تطوير واستخدام برامج مراقبة رقمية متقدمة أحد الوسائل الأساسية للكشف عن السلوكيات المسيئة على الإنترنت بشكل سريع وفعّال، فتُمكّن هذه البرامج هيئات الضبط الإداري الإلكتروني من رصد الأنشطة المشبوهة في الوقت الفعلي، مما يتيح لها اتخاذ إجراءات فورية قبل تفاقم الأضرار. ويمكن من خلال هذه الأدوات إرسال إنذارات رسمية عبر البريد الإلكتروني أو الرسائل النصية إلى الجناة المحتملين، تحذرهم من العواقب القانونية المحتملة وتوجههم إلى

---

[1] د. ياسر محمد اللمعي، المواجهة الجنائية لظاهرة التنمر الإلكتروني في ضوء السياسة التشريعية الحديثة، مرجع سابق، ص 139.

إيقاف سلوكياتهم على الفور، مما يعزز من فعالية التدابير الوقائية ويحد من انتشار التنمر الإلكتروني.

إلى جانب ذلك، تعمل هيئات الضبط الإداري الإلكتروني على توفير قنوات اتصال مباشرة لتمكين الضحايا والمواطنين من الإبلاغ عن حالات التنمر الإلكتروني بسهولة وسرعة، وقد تشمل هذه القنوات الخطوط الساخنة وتطبيقات الهاتف المحمول المخصصة لتلقي الشكاوى والبلاغات. ويمكن للهيئات من خلال هذه الآليات التعامل مع الحوادث بشكل فوري، وتقديم الدعم اللازم للضحايا، وضمان متابعة البلاغات بما يحقق الحماية المطلوبة ويعزز من استقرار وأمان البيئة الإلكترونية.

الفرع الثاني

التدابير العلاجية لهيئات الضبط الإداري لمكافحة التنمر الإلكتروني

قد لا تحقق التدابير الوقائية التي تتخذها هيئات الضبط الإداري الإلكتروني كامل أهدافها في منع وقوع جرائم التنمر الإلكتروني، مما يؤدي إلى عدم تحقق الردع الوقائي المطلوب. وفي هذه الحالات، يكون من الضروري أن تلجأ هذه الهيئات إلى تدابير علاجية لمعالجة الوضع، وقد تختلف هذه التدابير في شدتها بناءً على طبيعة الجريمة أو النشاط الذي قام به الأشخاص، وقد تصل هذه التدابير إلى تقييد بعض الحقوق والحريات، أو حتى إحالة المخالفين إلى القضاء المختص لاتخاذ الإجراءات القانونية بحقهم. ولهذا السبب، تحرص التشريعات دائمًا على تنظيم هذه المسألة بشكل يحقق التوازن الدقيق بين احترام حقوق وحريات الأفراد، وبين مكافحة جرائم التنمر الإلكتروني بفعالية، ومن أهم هذه التدابير ما يأتي:

أولًا: تقويم سلوك المتنمرين ودعم ضحايا التنمر الإلكتروني

يتوجب على هيئات الضبط الإداري الإلكتروني اتخاذ إجراءات شاملة تشمل إحالة الجاني المتنمر إلكترونيًا إلى مختص اجتماعي لتقويم سلوكه ومتابعة حالته النفسية، مع التوصية بالإجراءات اللازمة، بما في ذلك إمكانية إدخاله إلى مستشفى الأمراض النفسية والعقلية، إذا اقتضى الأمر[1].

[1] د. ياسر محمد اللمعي، المواجهة الجنائية لظاهرة التنمر الإلكتروني في ضوء السياسة التشريعية الحديثة، مرجع سابق، ص 137.

وعلاوة على ذلك، يتعين على هيئات الضبط الإداري الإلكتروني إنشاء وحدات أو برامج متخصصة تُعنى بتقديم الدعم الكامل لضحايا التنمر الإلكتروني؛ تشمل هذه الخدمات توفير المساعدة القانونية اللازمة لتمكين الضحايا من الدفاع عن حقوقهم وتوجيههم في الإجراءات القانونية المتبعة، بالإضافة إلى تقديم الدعم النفسي والاجتماعي اللازم للتعامل مع الأضرار الناجمة عن تلك الاعتداءات الإلكترونية، مما يعزز من قدرتهم على العودة إلى حياتهم الطبيعية دون أي تبعات نفسية أو عقلية تؤثر عليهم في المستقبل.

كما يتعين على هيئات الضبط الإداري الإلكتروني توفير قنوات متخصصة للإبلاغ عن حالات التنمر، مما يتيح للضحايا والشهود تقديم بلاغات فورية وسرية. وتشمل هذه القنوات منصات إلكترونية آمنة، وخطوط هاتفية مخصصة، وتطبيقات ذكية تُمكن المستخدمين من الإبلاغ بسرية تامة، مع توفير إرشادات واضحة حول الإجراءات الواجب اتباعها، إن هذه الآلية لا تقتصر على مجرد تلقي البلاغات، بل تمتد لتقديم الدعم الفوري للضحايا وضمان خصوصيتهم، مما يعزز من فعالية التدابير الوقائية ويؤكد التزام هيئات الضبط الإداري الإلكتروني بحماية الأفراد وتحقيق العدالة في البيئة الرقمية.

وقد نص التقرير النهائي للجنة الاقتصادية والاجتماعية الأوروبية، المقدم للبرلمان الأوروبي في 13 سبتمبر 2011، والمتعلق بحماية الأطفال والقاصرين في العالم الرقمي، على أهمية التعاون مع أصحاب المصلحة وتبني التنظيم الذاتي لمكافحة المحتوى غير القانوني أو الضار على مواقع التواصل الاجتماعي عبر الإنترنت. وأكد التقرير على ضرورة الالتزام بالضوابط المنصوص عليها في مدونات السلوك، مع التأكيد على الدول الأعضاء بضرورة تحديث هذه التدابير بشكل مستمر من خلال الرصد الدائم للسلوكيات الضارة، لضمان فعالية الإجراءات المتخذة. كما أشار التقرير إلى الالتزام بإنشاء خطوط ساخنة مباشرة للإبلاغ عن المحتوى الإلكتروني المسيء أو الضار. كما يتعين على الشركات القائمة على إدارة مواقع التواصل الاجتماعي، مثل فيسبوك وتويتر وإنستجرام، وغيرها من المنصات، استحداث خصائص ووظائف جديدة تُمكن من التصدي بشكل أكثر فعالية لظاهرة التنمر الإلكتروني، مما يعزز حماية المستخدمين في الفضاء الرقمي[1].

---

[1] Document de la commission COM (2011) 556 final du 13 septembre 2011, Rapport de la commission au parlement européen, au conseil, au comité économique et social européen et au comité des régions sur l'application de la recommandation du Conseil du 24 septembre 1998 concernant la protection des

ثانيًا: الإبلاغ عن المحتويات المخلة بالنظام العام على الشبكات الإلكترونية

في إطار تعزيز فعالية سلطات الضبط الإداري الإلكتروني في مواجهة التنمر الإلكتروني، تلعب هذه السلطات دورًا حيويًا في الإبلاغ عن المحتويات التي تخل بالنظام العام في الفضاء الرقمي، بالإضافة إلى الأساليب التقليدية المتبعة للإبلاغ عن الجرائم عبر مراكز الضبط القضائي وهيئات النيابة العامة. فيمكن للمستخدمين المشاركة بفعالية في ضبط هذا النوع من المحتوى على الشبكات الاجتماعية من خلال الإبلاغ عنه إلى السلطات العمومية المختصة المتواجدة على المنصات الرقمية، ويتم ذلك من خلال التواصل مع حسابات الجهات المختصة، مثل أجهزة الشرطة أو السلطات المعنية، على الشبكات الاجتماعية، أو عبر مواقع إلكترونية مخصصة لتلقي هذه البلاغات[1].

ثالثًا: إغلاق الأنشطة غير المرخصة

يمكن لهيئات الضبط الإداري الإلكتروني اتخاذ تدابير صارمة تشمل إغلاق الأنشطة التجارية أو المنظمات غير المرخصة التي يثبت تورطها في جرائم التنمر الإلكتروني، ويعد هذا الإجراء أداة فعّالة لتعزيز الرقابة على الأنشطة الإلكترونية وضمان الامتثال للتشريعات الوطنية. كما يتطلب التنسيق الوثيق مع شركات التكنولوجيا ومقدمي خدمات الإنترنت لإزالة المحتوى المسيء بشكل فوري، ومراقبة الأنشطة المشبوهة التي قد تنطوي على ممارسات التنمر الإلكتروني، وذلك لضمان بيئة إلكترونية آمنة تتوافق مع مبادئ النظام العام وحماية حقوق الأفراد.

رابعًا: التعاون مع المؤسسات التعليمية والتوعوية

يُعد التعاون مع المؤسسات التعليمية والتوعوية أحد المحاور الأساسية التي ينبغي على هيئات الضبط الإداري الإلكتروني تبنيها لتعزيز الجهود الوقائية والعلاجية. ويشمل هذا التعاون

---

mineurs et de la dignité humaine, et de la recommandation du Parlement européen et du Conseil du 20 décembre 2006 sur la protection des mineurs et de la dignité humaine et sur le droit de réponse en liaison avec la compétitivité de l'industrie européenne des services audiovisuels et d'information en ligne– Protéger les enfants dans le monde numérique, Dalloz, Paris, 2011.

[1] د. بلخير محمد آيت عودية، الضبط الإداري للشبكات الاجتماعية الإلكترونية، رسالة دكتوراة، كلية الحقوق والعلوم السياسية، جامعة باتنة (1)، الجزائر، 2018–2019م، ص 238، منشورة على الموقع الآتي:

- https://www.researchgate.net/publication/332683792.

العمل مع المدارس والجامعات ومؤسسات المجتمع المدني لتطوير وتنفيذ برامج إعادة التأهيل للجناة– لا سيما اليافعين منهم، بما يضمن توعيتهم بمخاطر التنمر الإلكتروني وأهمية الالتزام بالسلوك الأخلاقي في الفضاء الرقمي، كما تسعى هذه البرامج إلى إصلاح السلوكيات المنحرفة وتوجيه الأفراد نحو الاستخدام المسؤول للإنترنت، مما يسهم في الحد من تكرار الجرائم الإلكترونية وضمان بيئة إلكترونية أكثر أمانًا.

خامسًا: المصادرة

تُعتبر مصادرة الأدوات المستخدمة في ارتكاب جريمة التنمر الإلكتروني من التدابير العلاجية التي تتخذها هيئات الضبط الإداري الإلكتروني لمواجهة هذه الظاهرة؛ فيُنفذ هذا الإجراء بعد ثبوت ارتكاب الجريمة ويهدف إلى إزالة الأدوات التي كانت وسيلة الجاني في إلحاق الضرر بالمجني عليه، وبالتالي الحد من إمكانية تكرار الجريمة باستخدام نفس الوسائل. فمن خلال مصادرة هذه الأدوات، تسعى الهيئات إلى معالجة آثار الجريمة ومنع استمرار استخدامها في أفعال مشابهة، مما يجعل هذا الإجراء جزءًا من الاستجابة القانونية والتأديبية التي تركز على تقليل الأضرار الناجمة عن الجريمة بعد وقوعها، وضمان عدم تكرارها في المستقبل.

وتطبيقًا على ذلك، فقد نصت المادة (38) من القانون رقم 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات على أنه: "مع عدم الإخلال بحقوق الغير حسن النية، على المحكمة في حالة الحكم بالإدانة في أي جريمة من الجرائم المنصوص عليها في هذا القانون أن تقضي بمصادرة الأدوات والآلات والمعدات والأجهزة مما لا يجوز حيازتها قانونًا، أو غيرها مما يكون قد استخدم في ارتكاب الجريمة، أو سهل أو ساهم في ارتكابها.

وفي الحالات التي يتطلب فيها مزاولة النشاط الحصول على ترخيص من إحدى الجهات الحكومية، ولم يكن الشخص الاعتباري المدان بأي جريمة منصوص عليها في هذا القانون قد حصل على الترخيص، فيحكم عليه، فضلًا عن العقوبات المقررة، بالغلق".

وبذلك، جاءت المادة (38) من القانون رقم 175 لسنة 2018 بمجموعة من التدابير العلاجية التي تُمكّن هيئات الضبط الإداري الإلكتروني من مكافحة جرائم التنمر الإلكتروني بفعالية؛ أبرز هذه التدابير هو مصادرة الأدوات والآلات والمعدات والأجهزة التي تم استخدامها في ارتكاب الجريمة أو سهلت أو ساهمت في ارتكابها، مما يحد من قدرة الجناة على إعادة استخدام هذه الوسائل في المستقبل. كما تُلزم المادة المحكمة بالحكم بالغلق في حال كان النشاط يتطلب ترخيصًا ولم يحصل عليه الشخص الاعتباري المدان، مما يعزز من قوة الردع ضد

الجهات غير المرخصة التي تساهم في ارتكاب جرائم التنمر الإلكتروني. وتمثل هذه الإجراءات أدوات قانونية فعّالة تسهم في معالجة آثار الجريمة والحد من تكرارها، مع الحفاظ على حقوق الأطراف الأخرى حسنة النية.

الفرع الثالث

الصعوبات التي تواجه هيئات الضبط الإداري الإلكتروني في مواجهة التنمر الإلكتروني وكيفية التغلب عليها

تواجه هيئات الضبط الإداري الإلكتروني عدة تحديات أو صعوبات أثناء ممارسة اختصاصاتها في الكشف عن جريمة التنمر الإلكتروني وجمع الاستدلالات المتعلقة بها، وفيما يلي استعراض بعض هذه التحديات مع تقديم حلول مقترحة لمعالجتها بشكل فعال:

أولًا: صعوبة كشف الجريمة في بيئة الإنترنت

تتسم جريمة التنمر الإلكتروني بخصائص فريدة تجعل من الصعب كشفها في بيئة الإنترنت، حيث تختلف هذه الجرائم في طبيعتها عن الجرائم التقليدية. وترجع هذه الصعوبة إلى عاملين رئيسيين: الأول هو خفاء هذه الجرائم، والثاني هو إحجام الضحايا، خصوصًا في قطاع المال والأعمال، عن الإبلاغ عنها.

1- خفاء الجريمة:

تُعد جرائم الإنترنت، بما في ذلك التنمر الإلكتروني، من الجرائم التي غالبًا ما تتم في الخفاء، حيث يصعب على الضحايا إدراك وقوعها أو ملاحظتها. ويعود ذلك إلى مهارة الجناة ومعرفتهم الواسعة بكيفية إخفاء وحجب الأدلة المتعلقة بالأفعال الإجرامية، مما يجعل من الصعب تتبعهم واكتشاف جرائمهم[1].

2- الإحجام عن الإبلاغ:

يُشكل إحجام الأفراد والجهات المتضررة من جرائم الإنترنت عن الإبلاغ عنها تحديًا كبيرًا لهيئات الضبط الإداري الإلكتروني. ويعرقل هذا الإحجام جهود التحقيق والملاحقة، حيث تتردد

---

[1] د. هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية: دراسة مقارنة، مكتبة الآلات الحديثة، أسيوط، 1994م، ص 17.

العديد من المؤسسات والشركات في الإفصاح عن تعرضها لهذه الجرائم خوفًا من التأثير السلبي على سمعتها أو لتجنب تداعيات قانونية محتملة[1].

ولتعزيز فعالية هيئات الضبط الإداري الإلكتروني في مواجهة جرائم التنمر الإلكتروني، يتعين عليها الاستثمار في تقنيات متقدمة مثل الذكاء الاصطناعي وتحليل البيانات الضخمة لرصد السلوكيات المشبوهة وتحليل الأنماط والاتصالات التي قد تكشف عن النشاطات غير القانونية. وتساعد هذه التقنيات في كشف الجرائم التي يحاول الجناة إخفاءها وتسمح باتخاذ إجراءات استباقية.

كما يمكن تحسين الكشف عن الجرائم من خلال تشجيع الإبلاغ عبر حملات توعية مكثفة تستهدف المؤسسات والأفراد، مع التأكيد على سرية المعلومات المقدمة وتوفير آليات إبلاغ آمنة. ومن الضروري أيضًا إقامة شراكات استراتيجية مع شركات الأمن السيبراني والمنظمات غير الحكومية لدعم تطوير أدوات وتقنيات جديدة لمكافحة التنمر الإلكتروني. وأخيرًا، يجب توفير حوافز قانونية للمبلغين عن الجرائم وإنشاء وحدات متخصصة داخل الهيئات لتطوير مهارات وخبرات عالية في إدارة وكشف جرائم الإنترنت.

ثانيًا: عدم كفاية القوانين القائمة

في ظل التطور السريع الذي تشهده التكنولوجيا وازدياد الاعتماد عليها في مختلف جوانب الحياة العامة والخاصة، يواجه الجناة فرصة استغلال هذه التقنيات لارتكاب الجرائم، مما يبرز عدم كفاية النصوص القانونية الحالية في مواجهة الجرائم الإلكترونية الحديثة، ولا يتواكب التطور السريع في مجال المعلومات مع التطور المماثل في النصوص القانونية، حيث تقتصر القوانين الجنائية الحالية على تحديد الجريمة من خلال أدلة مادية ملموسة، وهو ما يتنافى مع الطبيعة الرقمية للجرائم الإلكترونية، وبالتالي قد تخرج بعض صور الجرائم من نطاق العقاب

ونتيجة لذلك، يتعين على هيئات الضبط الإداري الإلكتروني مواجهة التحديات التي تفرضها الجرائم غير الملموسة من خلال التكيف مع الأساليب الحديثة في الكشف والتحقيق، وتحديث المنظومات الإجرائية لتكون متوافقة مع المتطلبات العملية الإثباتية في مجال تقنية المعلومات والاتصالات. ويجب أن يتم هذا التحديث دون المساس بحقوق وحريات الأفراد، ويشمل تطوير

[1] د. هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مرجع سابق، ص 89.

أدوات وتقنيات متقدمة للتعامل مع الأدلة الرقمية وإجراء تحقيقات دقيقة تلائم طبيعة الجرائم الإلكترونية[1].

كما ينبغي على هيئات الضبط الإداري الإلكتروني العمل بالتنسيق مع الجهات التشريعية لمراجعة وتحديث الأطر القانونية القائمة، بما يكفل استيعاب الطبيعة الرقمية للجرائم الإلكترونية. ويتضمن ذلك صياغة قوانين جديدة أو تعديل القوانين القائمة لتشمل الجرائم ذات الطابع الرقمي، مع تحديد واضح للأدلة الرقمية والاعتراف بها كأدلة قانونية ذات حجية في الإجراءات القضائية.

ثالثًا: نقص خبرة سلطات الضبط الإداري

من أبرز التحديات التي تواجه سلطات الضبط الإداري الإلكتروني في مواجهة جرائم التنمر الإلكتروني نقص الكفاءة والخبرة اللازمة لدى العاملين في هذا المجال، مما يعوق قدرتهم على التصدي لهذه الجرائم المتطورة. ورغم الجهود المبذولة لاستيعاب المختصين في مجال الحاسوب والإنترنت ضمن كوادر هذه الهيئات، وتدريب العاملين على استخدام التقنيات الحديثة، فإن هذه الجهود لا تزال غير كافية لمواكبة التطور السريع في هذا المجال.

وتعزى هذه الصعوبة إلى عدة أسباب، منها: ضعف الميزانيات المخصصة لتدريب الكوادر البشرية واستقطاب الخبراء المتميزين في مجال الحاسوب، الذين غالبًا ما يتم استقطابهم من قبل شركات القطاع الخاص. بالإضافة إلى حداثة تجربة هذه الهيئات في التعامل مع الجرائم الإلكترونية، وضعف الخبرة الفنية والإجرائية لديها، مما يؤدي إلى قلة عدد الجرائم المكتشفة وضعف القدرة على التحقيق فيها[2].

وبناءً على ذلك، يتوجب على سلطات الضبط الإداري الإلكتروني تعزيز إمكاناتها التقنية وتطوير قدراتها البشرية لمواجهة جرائم التنمر الإلكتروني بفعالية. وينبغي العمل على استقطاب الكفاءات المتخصصة في هذا المجال والاستعانة بالخبراء في مراحل التحقيق وجمع الأدلة، لضمان تحقيق العدالة في هذه الجرائم المعقدة.

ويبرز هنا أيضًا أهمية التدريب الفني المتخصص لجهات الضبط الإداري الإلكتروني، بما في ذلك الجهات المعنية بالتحقيق والقضاء، على استخدامات وتطبيقات الحاسوب والإنترنت،

---

[1] د. محمد منير صالح وآخرون، الجرائم المعلوماتية وطرق مواجهتها، مركز بحوث الشرطة، أكاديمية الشرطة، الإصدار الثالث، 2000م، ص 179.

[2] للمزيد من التفصيل يراجع: د. سامح أحمد بلتاجي، الجوانب الإجرائية للحماية الجنائية لشبكة الإنترنت، رسالة دكتوراة، كلية الحقوق، جامعة الإسكندرية، 2010م، ص 224.

وسبل مواجهة الجرائم التي تقع ضمن نطاق هذه التقنيات التكنولوجية المتطورة. فعملية اكتساب الخبرة في مجال جرائم تقنية المعلومات يعد أمرًا بالغ الأهمية؛ حيث إن قدرة رجال الضبط والمحققين على القيام بواجباتهم في جمع الاستدلالات والتحقيق تعتمد بشكل كبير على إلمامهم بتقنيات الحاسب الآلي، وبدون هذا الإلمام قد تصبح عملية مواجهة جرائم التنمر الإلكتروني غير فعالة، مما يؤكد ضرورة توفير التدريب اللازم والمتخصص لهذه الجهات لضمان تحقيق العدالة ومكافحة الجرائم الإلكترونية بفعالية[1].

رابعًا: صعوبة إثبات جريمة التنمر الإلكتروني والتحقيق فيها

تواجه سلطات الضبط الإداري الإلكتروني تحديات كبيرة في إثبات جريمة التنمر الإلكتروني والتحقيق فيها؛ نظرًا لعدد من الصعوبات المميزة لهذا النوع من الجرائم، تتمثل هذه الصعوبات في: انعدام الأثر المادي، حيث لا يتخلف عن الجريمة أي دليل كتابي، ويمكن للجاني تدمير أدلة الإدانة في لحظات. كما تتضمن الصعوبات غياب الدليل المرئي، وإمكانية إخفاء الجريمة بطرق تقنية، واستخدام وسائل الحماية الفنية التي تعيق الوصول إلى الأدلة. بالإضافة إلى ذلك، تشكل ضخامة البيانات التي يتعين فحصها تحديًا كبيرًا، إلى جانب إحجام الأفراد والشركات عن الإبلاغ عن الجرائم الإلكترونية للحفاظ على ثقة العملاء. كما أن نقص خبرة رجال الشرطة وجهات الادعاء والقضاء في هذا المجال، وإمكانية ارتكاب الجريمة من مسافات بعيدة تتجاوز الحدود الوطنية، يزيدان من تعقيد مهمة مكافحة هذه الجرائم[2].

ولمواجهة التحديات التي تفرضها ضخامة كم البيانات والمعلومات التي يتعين على سلطات الضبط الإداري الإلكتروني تحليلها لاستخلاص الأدلة على ارتكاب جريمة التنمر الإلكتروني، يمكن تقليص حدة هذه الصعوبات وتيسير التعامل معها من خلال اتباع وسيلتين أساسيتين:

الوسيلة الأولى: الاستعانة بالخبرة الفنية المتخصصة لتحديد البيانات والمعلومات ذات الصلة بالجريمة بشكل دقيق، مما يساهم في توجيه جهود البحث والتحليل نحو ما يجب الاطلاع عليه أو ضبطه دون إضاعة الوقت والموارد على بيانات غير ذات صلة.

---

[1] د. فوزي محمد صقر، تدابير الضبط الإداري لمكافحة جرائم وسائل التواصل الاجتماعي، مجلة مصر المعاصر، المجلد 111، العدد 540، الجمعية المصرية للاقتصاد السياسي والإحصاء والتشريع، القاهرة، أكتوبر 2020م، ص 528-529.

[2] أ. عماد جاسم محمد الشنكالي، دور الضبط الإداري الإلكتروني في مكافحة الجرائم المعلوماتية، مرجع سابق، ص 139.

الوسيلة الثانية: الاستفادة من نظم المعالجة الآلية للبيانات التي توفر أساليب متقدمة للتدقيق والفحص المنهجي، بالإضافة إلى أدوات الاختيار والمراجعة، فتتيح هذه النظم إمكانية الفحص الدقيق للحالات أو الوقائع المعنية، مما يسهل عملية استخلاص الأدلة بشكل أكثر فعالية ودقة[1].

خامسًا: الاختلافات القانونية بين الدول

تعد الاختلافات القانونية بين الدول من أبرز التحديات التي تواجه هيئات الضبط الإداري الإلكتروني في مواجهة جرائم التنمر الإلكتروني؛ إذ إن الجرائم الإلكترونية غالبًا ما تتجاوز الحدود الوطنية، مما يعقد عملية التصدي لها عندما يكون الجاني في دولة أخرى تخضع لقوانين مختلفة أو عندما تفتقر تلك الدول إلى اتفاقيات تعاون مشترك لمكافحة هذا النوع من الجرائم.

وللتغلب على التحديات التي تفرضها الاختلافات القانونية بين الدول في مواجهة جرائم التنمر الإلكتروني، يتعين على هيئات الضبط الإداري الإلكتروني اتباع عدة خطوات استراتيجية، منها:

1- يجب تعزيز التعاون الدولي من خلال إبرام اتفاقيات ثنائية ومتعددة الأطراف مع الدول الأخرى، تركز على مكافحة الجرائم الإلكترونية بشكل شامل، وينبغي أن تتضمن هذه الاتفاقيات آليات واضحة لتبادل المعلومات والأدلة، وتنسيق الجهود بين الجهات المختصة في كل دولة، بما يتيح ملاحقة الجناة عبر الحدود دون عوائق قانونية.
2- يجب أن تعمل هيئات الضبط الإداري الإلكتروني على تطوير شراكات مع المنظمات الدولية المتخصصة في مكافحة الجرائم الإلكترونية، مثل الإنتربول واليوروبول، لتعزيز قدرتها على مواجهة الجرائم العابرة للحدود، ويمكن لهذه الشراكات أن تسهم في تقديم الدعم الفني وتسهيل التعاون القضائي بين الدول.
3- يتعين على الهيئات المعنية الاستثمار في برامج تدريبية مكثفة لموظفيها على القوانين الدولية المتعلقة بالجرائم الإلكترونية، واطلاعهم على أفضل الممارسات العالمية في هذا المجال، فهذا التدريب يمكن أن يساعد في تجاوز التحديات القانونية وتعزيز فعالية التحقيقات والإجراءات القضائية.

---

[1] د. هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مرجع سابق، ص 24؛ د. فوزي محمد صقر، تدابير الضبط الإداري لمكافحة جرائم وسائل التواصل الاجتماعي، مرجع سابق، ص 530.

الخاتمة

في خاتمة هذا البحث، نستعرض أهم النتائج المستخلصة، ونقدم بعض التوصيات المستندة إلى ما توصلنا إليه من خلال الدراسة المتعمقة لهذا الموضوع الجوهري، وذلك على النحو الآتي:

أولًا: النتائج

1- يُعرَّف التنمر الإلكتروني بأنه سلوك عدواني متعمد ومتكرر يتم ارتكابه باستخدام وسائل الإعلام الإلكترونية أو الرقمية، ويُنفَّذ بواسطة فرد أو مجموعة، وغالبًا ما يتوارى المتنمرون خلف هويات مزيفة أو مجهولة. ويهدف هذا السلوك إلى إلحاق الأذى النفسي، أو الجسدي، أو الاجتماعي بالضحية، وذلك من خلال استخدام أساليب التحرش اللفظي، والتهديد، والتلاعب، ونشر الشائعات الخبيثة، والتمييز على أساس العرق أو الدين، والإذلال العلني. ويتمتع التنمر الإلكتروني بقابلية واسعة للانتشار السريع واستمرارية التأثير لفترات طويلة، مما قد يؤدي إلى آثار نفسية واجتماعية خطيرة على الضحية، تشمل القلق، والاكتئاب، والعزلة الاجتماعية، وتدهور الأداء الأكاديمي أو المهني، وقد يصل الأمر إلى حد دفع الضحية للانتحار.

2- يتضمن التنمر الإلكتروني العديد من الصور والأشكال التي يقوم المتنمر من خلالها بإلحاق الأذى والضرر المتعمد بالضحية باستخدام الوسائل التكنولوجية الحديثة، ومن أبرز هذه الصور: التنمر عبر الرسائل النصية أو البريد الإلكتروني، والتنمر بنشر الشائعات عبر الإنترنت، والتنمر بالمضايقات في غرف الدردشة ومواقع التواصل الاجتماعي، والتنمر عبر قرصنة الحسابات وسرقة الهوية الرقمية، والتنمر باستخدام الأسماء المستعارة، والتنمر بواسطة الصور ومقاطع الفيديو، والتنمر من خلال المحتوى الجنسي، والتنمر عبر المطاردة أو الملاحقة الإلكترونية.

3- إن مواجهة جريمة التنمر الإلكتروني من قِبَل هيئات الضبط الإداري تُعد مهمة شديدة التعقيد، ولا يمكن تنفيذها بالشكل الأمثل إلا إذا كانت تلك الهيئات مزودة بالأدوات والوسائل اللازمة لأداء هذه المهمة بشكل يحقق الأهداف المنشودة، وبما يضمن أن تكون الإجراءات المتخذة مشروعة ومتوافقة مع المبادئ والقواعد المنظمة لحقوق الإنسان وحرياته. كما يتعين على هذه الهيئات الالتزام التام بالواجبات الموكلة إليها بموجب القوانين والأنظمة والتعليمات النافذة، دون المساس بتلك الواجبات أو تجاوز حدودها. ولا تختلف الوسائل المستخدمة في الضبط الإداري الإلكتروني في طبيعتها وضوابط مشروعية استخدامها عن تلك المعتمدة في الضبط الإداري التقليدي.

4- تتولى هيئات الضبط الإداري الإلكتروني المختصة بمكافحة التنمر الإلكتروني اتخاذ مجموعة من الإجراءات المتنوعة التي تهدف إلى مكافحة هذا النوع من الجرائم الإلكترونية، وتختلف هذه الإجراءات وفقًا لطبيعة التدخل المطلوب؛ حيث إن بعض هذه الإجراءات يتسم بالطابع الوقائي، إذ يتم اتخاذه قبل مباشرة الأفراد لأي نشاط قد يؤدي إلى وقوع جريمة التنمر الإلكتروني، وذلك بهدف الحيلولة دون وقوعها، في حين تتسم الإجراءات الأخرى بالطابع العلاجي، إذ تهدف إلى معالجة الأفعال التي قد تُصنَّف ضمن جرائم التنمر الإلكتروني بعد وقوعها.

5- تواجه هيئات الضبط الإداري الإلكتروني العديد من التحديات والصعوبات أثناء ممارسة اختصاصاتها في الكشف عن جريمة التنمر الإلكتروني وجمع الاستدلالات المرتبطة بها، ومن أبرز هذه التحديات: صعوبة رصد الجريمة في بيئة الإنترنت، وعدم كفاية التشريعات القائمة لمواكبة التطورات التقنية، ونقص الخبرات المتخصصة لدى سلطات الضبط الإداري الإلكتروني، بالإضافة إلى تعقيدات إثبات جريمة التنمر الإلكتروني، والاختلافات القانونية بين الدول التي تعيق التعاون الدولي في هذا المجال.

6- يُعتبر التشريع المصري أفضل من نظيره الفرنسي في مواجهة جريمة التنمر؛ نظرًا لشمولية نصوصه التي توفر تغطية قانونية أوسع لا تقتصر على بيئات معينة، بل تمتد لتشمل جميع الحالات التي قد يقع فيها التنمر، مما يعزز قدرة القانون على حماية كافة الفئات المتضررة. كما يتميز التشريع المصري بالمرونة في تحديد العقوبة؛ حيث منح المشرع للقاضي سلطة تقديرية واسعة لاختيار العقوبة المناسبة بين الحبس والغرامة أو الجمع بينهما، بما يتيح تكييف العقوبة وفقًا لخطورة الجريمة وظروف المتهم الشخصية. إضافة إلى ذلك، يميز التشريع المصري بين الحالات العادية والمشددة للتنمر، مع تشديد العقوبة في الحالات التي تتطلب ذلك، مما يعكس وعي المشرع بخطورة بعض أشكال التنمر وضرورة مواجهتها بعقوبات أكثر صرامة.

ثانيًا: التوصيات

1- تعزيز التعاون الدولي بين الدول لمواجهة الطبيعة العابرة للحدود للتنمر الإلكتروني، ويقترح إنشاء منصات دولية مشتركة لتبادل المعلومات والخبرات بين هيئات الضبط الإداري في مختلف الدول، مما يسهم في التصدي الفوري للجرائم الرقمية التي تتجاوز الحدود الوطنية. بالإضافة إلى ذلك، نوصي بتبني سياسات تركز على التوعية المجتمعية والتثقيف الرقمي، لا سيما بين الشباب والأطفال؛ لتعزيز الوعي بمخاطر التنمر الإلكتروني وكيفية مواجهته، مما يساهم في الحد من انتشار هذه الظاهرة في المجتمع.

2- تبرز الحاجة الملحة لوضع تشريع خاص لمواجهة ظاهرة التنمر الإلكتروني بكافة أشكالها؛ نظرًا لكونها ظاهرة إجرامية إلكترونية مستحدثة تتطلب معاملة قانونية وإجرائية تختلف عن الجرائم التقليدية. ورغم أن المشرع المصري قد اتخذ خطوة إيجابية في 5 سبتمبر 2020 بإضافة المادة 309 مكررًا (ب) إلى قانون العقوبات لتجريم التنمر، إلا أن خطورة هذه الظاهرة وتأثيرها العميق على استقرار المجتمع تستدعي تدخلًا تشريعيًا أوسع، فيتعين على المشرع المصري أن يضع قانونًا خاصًا يشمل تجريم كافة صور التنمر، سواء التقليدي منها أم الإلكتروني، لضمان حماية المجتمع بشكل أكثر شمولية وفعالية، وتعزيز قدرة سلطات الضبط الإداري الإلكتروني على مواجهة هذه الجرائم المستحدثة بفعالية أكبر.

3- نوصي بضرورة اعتماد إجراءات قانونية مرنة وسريعة تُمكّن الضحايا من تقديم شكاواهم ضد مرتكبي جريمة التنمر الإلكتروني دون تعقيدات أو تأخير، مع ضمان حماية صارمة لسرية المعلومات الشخصية الخاصة بالضحايا والشهود، فمثل هذه الضمانات تعد أساسية لتوفير بيئة آمنة تشجع الأفراد المتضررين على الإبلاغ عن حالات التنمر دون خوف من التعرض لأي نوع من الانتقام أو الأذى، مما يعزز من فعالية العدالة ويضمن احترام حقوق الإنسان.

4- يتعين على سلطات الضبط الإداري الإلكتروني تنظيم سلسلة من المؤتمرات المتخصصة التي تهدف إلى نشر الوعي الثقافي حول مخاطر التنمر الإلكتروني وآثاره السلبية على الأفراد والمجتمع، وينبغي أن تجمع هذه المؤتمرات بين الخبراء في المجالات القانونية، والتقنية، والاجتماعية، لتقديم رؤى شاملة حول كيفية الوقاية من هذه الظاهرة والتصدي لها بفعالية. كما يجب أن تتضمن هذه الفعاليات برامج توعية تستهدف مختلف فئات المجتمع، لتعزيز ثقافة الاستخدام المسؤول للإنترنت وتشجيع السلوكيات الإيجابية التي تدعم بيئة رقمية آمنة ومستقرة.

5- يُقترح إنشاء لجنة وطنية متخصصة لمكافحة ظاهرة التنمر الإلكتروني، تكون مهمتها وضع السياسات العامة اللازمة لمواجهة كافة أشكال التنمر الإلكتروني، كما تُعنى هذه اللجنة بمراجعة القوانين القائمة، وتحديد النصوص التي تستدعي التعديل أو التحديث لتكون أكثر فعالية في التصدي لهذه الظاهرة الإجرامية. بالإضافة إلى ذلك، ستتولى اللجنة اقتراح التدابير الاحترازية اللازمة للوقاية من الخطورة الإجرامية التي تمثلها ظاهرة التنمر الإلكتروني، مما يعزز من قدرة سلطات الضبط الإداري الإلكتروني على حماية المجتمع وضمان استقرار البيئة الرقمية.

قائمة المراجع

أولًا: المراجع القانونية العامة

1. توفيق شحاتة، مبادئ القانون الإداري، الطبعة الأولى، دار النشر للجامعات المصرية، القاهرة، 1955م.
2. جمال مطلق الذنيات، الوجيز في القانون الإداري، الدار العلمية الدولية، عمَّان، الأردن، 2003م.
3. سليمان محمد الطماوي، الوجيز في القانون الإداري، دار الفكر العربي، القاهرة، 1994م.
4. طعيمة الجرف، القانون الإداري والمبادئ العامة في تنظيم ونشاط السلطات الإدارية، دار النهضة العربية، القاهرة، 1978م.
5. ماجد راغب الحلو، القانون الإداري، دار المطبوعات الجامعية، الإسكندرية، 2000م.
6. مازن ليلو راضي، القانون الإداري، منشورات الأكاديمية العربية في الدنمارك، الدنمارك، 2008م.
7. محمد أنس جعفر، عبد المجيد عبد الحفيظ سليمان، أصول القانون الإداري، دار النهضة العربية، القاهرة، 2004م.
8. محمد رفعت عبد الوهاب، مبادئ وأحكام القانون الإداري، منشورات الحلبي الحقوقية، بيروت، لبنان، 2002م.
9. مصطفى معوض، أكرم أبو حساب، الموسوعة الجنائية للتشريعات الاقتصادية، الطبعة الأولى، طبعة خاصة بنادي القضاة، القاهرة، 2009م.
10. المكتب الفني لمجلس الدولة، مجموعة المبادئ القانونية التي قررتها المحكمة الإدارية العليا، السنة الثالثة عشرة، العدد الأول من أول أكتوبر سنة 1967 إلى منتصف فبراير 1968.
11. هاني علي الطهراوي، القانون الإداري، الكتاب الأول، الطبعة الأولى، مكتبة دار الثقافة للنشر والتوزيع، عمَّان، الأردن، 2001م.

ثانيًا: المراجع القانونية المتخصصة

1. أحمد محمد عبد الباقي، التكنولوجيا وجرائم المستقبل، الطبعة الأولى، دار النهضة العربية، القاهرة، 2017م.
2. أحمد محمد عبد الرؤوف المنيفي، التنمر وابتزاز النساء عبر الإنترنت، مركز الكتاب الأكاديمي، القاهرة، 2020م.

3. جميل عبد الباقي الصغير، جرائم الإنترنت: الأحكام الموضوعية والجوانب الإجرائية، طبعة خاصة بنادي القضاة، القاهرة، 2011م.
4. حلمي الدقدوقي، رقابة القضاء على المشروعية الداخلية لأعمال الضبط الإداري: دراسة مقارنة، دار المطبوعات الجامعية، الإسكندرية، 2004م.
5. خولة مرتضوي، ريشة حبر، بلاتينيوم بوك للنشر والتوزيع، قطر، 2016م.
6. رمضان محمد بطيخ، الاتجاهات المتطورة في قضاء مجلس الدولة الفرنسي للحد من سلطة الإدارة التقديرية وموقف مجلس الدولة المصري منها، دار النهضة العربية، القاهرة، 1994م.
7. سامي جمال الدين، قضاء الملاءمة والسلطة التقديرية للإدارة، دار النهضة العربية، القاهرة، 1992م.
8. سحر فؤاد مجيد، الجرائم المستحدثة: دراسة معمقة ومقارنة في عدة جرائم، الطبعة الأولى، المركز العربي للنشر والتوزيع، القاهرة، 2019م.
9. سعيد جبر، الحق في الصورة، دار النهضة العربية، القاهرة، 1986م.
10. سليمان محمد الطماوي، القضاء الإداري: قضاء التعويض وطرق الطعن في الأحكام- دراسة مقارنة، دار الفكر العربي للطباعة والنشر، القاهرة، 1986م.
11. سليمان محمد الطماوي، النظرية العامة للقرارات الإدارية: دراسة مقارنة، دار الفكر العربي، القاهرة، 1984م.
12. صلاح يوسف عبد العليم، أثر القضاء الإداري على النشاط الإداري للدولة، دار الفكر العربي، الإسكندرية، 2008م.
13. طارق فتح الله خضر، دعوى الإلغاء، دار النهضة العربية، القاهرة، 2002م.
14. علي موسى الصبحين، محمد فرحان القضاة، سلوك التنمر عند الأطفال والمراهقين (مفهومه- أسبابه- علاجه)، جامعة نايف العربية للعلوم الأمنية، الرياض، 2013م.
15. عمر الشريف، شرح مبادئ وأحكام قوانين الاتصالات، الطبعة الأولى، كلية الهندسة، جامعة الإسكندرية، 2008م.
16. محمد منير صالح وآخرون، الجرائم المعلوماتية وطرق مواجهتها، مركز بحوث الشرطة، أكاديمية الشرطة، الإصدار الثالث، 2000م.
17. محمود عاطف البنا، حدود سلطة الضبط الإداري، كلية الحقوق، جامعة القاهرة، 1980م.
18. ناجح أحمد عبد الوهاب، التطور الحديث للقانون الإداري في ظل نظام الحكومة الإلكترونية، دار النهضة العربية، القاهرة، 2012م.

19. ناصر لباد، القانون الإداري: النشاط الإداري، الطبعة الأولى، المكتبة الوطنية الجزائرية، الجزائر، 2004م.
20. هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية: دراسة مقارنة، مكتبة الآلات الحديثة، أسيوط، 1994م.

ثالثًا: المعاجم

1. أحمد مختار عمر، معجم اللغة العربية المعاصرة، الطبعة الأولى، دار عالم الكتب، القاهرة، 2008م.
2. عدنان أبو مصلح، معجم علم الاجتماع، مكتبة العبدلي، عمَّان، الأردن، 2010م.

رابعًا: الرسائل العلمية

1. بلخير محمد آيت عودية، الضبط الإداري للشبكات الاجتماعية الإلكترونية، رسالة دكتوراة، كلية الحقوق والعلوم السياسية، جامعة باتنة (1)، الجزائر، 2018-2019م، منشورة على الموقع الآتي: https://www.researchgate.net/publication/33268379
2. ثروت عبد العال أحمد، الرقابة القضائية على ملاءمة القرارات الإدارية، رسالة دكتوراة، كلية الحقوق، جامعة أسيوط، 1991م.
3. سامح أحمد بلتاجي، الجوانب الإجرائية للحماية الجنائية لشبكة الإنترنت، رسالة دكتوراة، كلية الحقوق، جامعة الإسكندرية، 2010م.
4. سعدية صالحي، مستوى التنمر المدرسي لدى التلاميذ: دراسة ميدانية على تلاميذ السنة الثالثة والرابعة متوسط بولايتي البيض وسعيدة، رسالة ماجستير، كلية العلوم الاجتماعية والإنسانية، قسم العلوم الاجتماعية، جامعة د. مولاي الطاهر سعيدة، الجزائر، 2017-2018م، منشورة على الموقع الآتي: https://bussh.univ-saida.dz/doc_num.php?explnum_id=1337.
5. عماد جاسم حسين الشنكالي، دور الضبط الإداري الإلكتروني في مكافحة الجرائم المعلوماتية: دراسة مقارنة، رسالة ماجستير، كلية الحقوق، جامعة تكريت، العراق، 2022م.
6. عمر بو قريط، الرقابة القضائية على تدابير الضبط الإداري، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة منتوري، قسنطينة، الجزائر، 2006-2007م، بحث منشور على الموقع الآتي: https://lib.manaraa.com/books.

7. فاطمة زهراء صوفي، المناخ المدرسي وعلاقته بالتنمر المدرسي لدى تلاميذ المرحلة الثانوية: دراسة ميدانية على عينة من تلاميذ التانوي بسعيدة، رسالة ماجستير، كلية العلوم الاجتماعية والإنسانية، قسم العلوم الاجتماعية، جامعة د. مولاي الطاهر سعيدة، الجزائر، 2017-2018م، منشورة على الموقع الآتي: https://bussh.univ-saida.dz/doc_num.php?explnum_id=1525.
8. فيصل كامل إسماعيل، سلطات الضبط الإداري أثناء حالة الطوارئ في مصر وفرنسا والولايات المتحدة الأمريكية، رسالة دكتوراة، كلية الحقوق، جامعة المنصورة، 2006م.
9. محمد شريف إسماعيل، الضبط الإداري في الظروف الاستثنائية، رسالة دكتوراة، كلية الحقوق، جامعة عين شمس، 1979م.
10. محمد فريد سليمان، الرقابة القضائية على التناسب في القرار الإداري، رسالة دكتوراة، كلية الحقوق، جامعة المنصورة، 1989م.
11. مهند قاسم زغير، السلطة التقديرية للإدارة في مجال الضبط الإداري في الظروف العادية: دراسة مقارنة في القانون الوضعي والشريعة الإسلامية، رسالة دكتوراة، كلية الحقوق، جامعة النهرين، بغداد، 2014م، منشورة على الموقع الآتي: https://nahrainuniv.edu.iq/sites/default/files/nwee%20old.pdf.

خامسًا: الدوريات والمؤتمرات

1. أحمد فكري بهنساوي، رمضان علي حسن، التنمر المدرسي وعلاقته بدافعية الإنجاز لدى تلاميذ المرحلة الإعدادية، مجلة كلية التربية، العدد (17)، جامعة بورسعيد، يناير 2015م.
2. ثناء هاشم محمد، واقع ظاهرة التنمر الإلكتروني لدى طلاب المرحلة الثانوية في محافظة الفيوم وسبل مواجهتها: دراسة ميدانية، مجلة جامعة الفيوم للعلوم التربوية والنفسية، العدد الثاني عشر، الجزء الثاني، 2019م.
3. حسين بن سعيد الغافري، جريمة التنمر الإلكتروني عبر وسائل التواصل الاجتماعي، مجلة روح القوانين، المجلد 35، العدد 103، كلية الحقوق، جامعة طنطا، يوليو 2023م.
4. حسين مقداد عبد اللطيف، دور الضبط الإداري في الحد من مخاطر الفضاء الإلكتروني في مصر وفرنسا، مجلة العلوم القانونية والاقتصادية، العدد الأول، السنة الخامسة والستون، كلية الحقوق، جامعة عين شمس، يناير 2023م.
5. رمزي طه الشاعر، المسؤولية عن أعمال السلطة القضائية، مجلة العلوم القانونية والاقتصادية، المجلد (18)، العدد (2)، كلية الحقوق، جامعة عين شمس، يوليو 1976م.

6. سليمة سايحي، أسماء سايحي، البرامج العالمية لمكافحة التنمر المدرسي: برنامج دان ألويس نموذجًا، المجلة الدولية للدراسات التربوية والنفسية، العدد 4، المركز الديمقراطي العربي ببرلين، ألمانيا، مارس 2019م، منشور على الموقع الآتي: https://democraticac.de/wp-content/uploads/2019/03/.
7. عمر محمد بن يونس، الحقوق والحريات والالتزامات الرقمية في الفقه المقارن، المؤتمر الإقليمي العربي "نحو مجتمع معلومات أكثر عدالة"، خلال الفترة من 13-15 سبتمبر 2004م، عمَّان، الأردن.
8. عمرو محمد محمد درويش، أحمد حسن محمد الليثي، فاعلية بيئة تعلم معرفي سلوكي قائمة على المفضلات الاجتماعية في تنمية استراتيجيات مواجهة التنمر الإلكتروني لطلاب المرحلة الثانوية، مجلة العلوم التربوية، المجلد 25، العدد الرابع، الجزء الأول، كلية الدراسات العليا للتربية، جامعة القاهرة، أكتوبر 2017م.
9. فوزي محمد صقر، تدابير الضبط الإداري لمكافحة جرائم وسائل التواصل الاجتماعي، مجلة مصر المعاصر، المجلد 111، العدد 540، الجمعية المصرية للاقتصاد السياسي والإحصاء والتشريع، القاهرة، أكتوبر 2020م.
10. كمال سيد عبد الحليم، جريمة التنمر وعقوبتها في الشريعة والقانون، مجلة كلية الشريعة والقانون، العدد الرابع والثلاثون، الإصدار الأول، جامعة الأزهر، فرع أسيوط، يناير 2022م.
11. محمد سليمان شبير، الإطار القانوني لسلطة الضبط الإداري الإلكتروني في فلسطين: دراسة تحليلية، مجلة جامعة الأزهر، المجلد 17، العدد 2 (ب)، غزة، فلسطين، 2015م، بحث منشور على الموقع الآتي:
   - https://www.researchgate.net/profile/Mohammed-Shbair.
12. محمد علي حسونة، حدود سلطات الضبط الإداري وأثرها على الحريات العامة، المجلة القانونية، المجلد 14، العدد 1، كلية الحقوق، جامعة القاهرة، نوفمبر 2022م.
13. محمود سعد الدين الشريف، أساليب الضبط الإداري والقيود الواردة عليه، مجلة مجلس الدولة المصري، السنة الثانية عشرة، 1964م.
14. مشعل الأسمر البنتان، العوامل الاجتماعية المؤدية لسلوك التنمر لتلاميذ المرحلة المتوسطة بمنطقة حائل: دراسة من منظور الممارسة العامة في الخدمة الاجتماعية، مجلة كلية التربية الأساسية للعلوم التربوية والإنسانية، العدد (42)، جامعة بابل، العراق، فبراير 2019م، منشور على الموقع الآتي: https://search.emarefa.net/ar/detail/BIM-893716.

15. معاوية محمود أبو غزال، الاستقواء وعلاقته بالشعور والوحدة والدعم الاجتماعي، المجلة الأردنية في العلوم التربوية، المجلد الخامس، العدد الثاني، كلية التربية، جامعة اليرموك، إربـــد، الأردن، 2009م، منشـــور علـــى الموقـــع الآتـــي:
https://journals.yu.edu.jo/jjes/Issues/2009/Vol5No2/art1.pdf
16. ندا منعم محمود السيد سلام، مدى كفاية التشريعات لمكافحة جريمة التنمر الإلكتروني: دراسة مقارنة، مجلة البحوث الفقهية والقانونية، العدد الحادي والأربعين، كلية الشريعة والقانون بدمنهور، جامعة الأزهر، إبريل 2023م.
17. نعيم عطية، حرمة الحياة الخاصة في القانونين المصري والفرنسي، مجلة العلوم الإدارية، المعهد الدولي للعلوم الإدارية، الشعبة المصرية، السنة 23، االمجلد 22، العدد الأول، القاهرة، يونية 1980م.
18. ياسر محمد اللمعي، المواجهة الجنائية لظاهرة التنمر الإلكتروني في ضوء السياسة التشريعية الحديثة: دراسة تحليلية مقارنة، مجلة روح القوانين، العدد الخامس والتسعون، كلية الحقوق، جامعة طنطا، يوليو 2021م.
19. يوسف ناصر حمد الظفيري، الضبط الإداري وحدود سلطاته في الظروف العادية والظروف الاستثنائية، مجلة البحوث القانونية والاقتصادية، المجلد 10، العدد 74، كلية الحقوق، جامعة المنصورة، ديسمبر 2020م.

سادسًا: المراجع الأجنبية

1. AJ FAM, Loi sur les violences sexistes et sexuelles, Dalloz, Paris, 2018.
2. Beran, T., & Li.Q., The relationship between cyberbullying and school bulling, The Journal of Student Wellbeing, 1 (2),2008.
3. BRIAN H.SPITZBERG, GREGORY HOOBLER, Clberstalking and the technologies of interpersonal terrorism new media & society, 2012, (1)4. see:
4. Bulach, C. Impiementing a character education cuiriculum and assessing its impact on ctud ent behavior. The clearing 2002.
5. CASTAGNE (J.) Le controle juridictonnel de la legalite des actes de police administrative "th, paris, 1961, Bordeaux, ed 1964.

6. Dalloz, Police administrative, Juillet 2021. https://www.dalloz.fr/documentation/Document.
7. De laubadere- Traite da droit administrative. LOI 1062-2001 du 15 novembre 2001 relative à la sécurité quotidienne, JORF n°266 du 16 novembre 2001 Texte n° 1; https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000000222052.
8. ECLAC: The new digital revolution; From the consumer Internet to the industrial Internet, the fifth Ministerial Conference on the Information Society in Latin America and the Caribbean, held in Mexico City from tov August ,2015.
9. Emily A. Vogels, Teens and Cyberbullying 2022: https://www.pewresearch.org/internet/2022/12/15/teens-and-cyberbullying-2022/.
10. ERIC Digest, Banks R.Bullying in school, Washington, DC:U.S.Department of Education and Justice.1997.
11. (E) Picard, la nation de police administrative, thèse, Paris I, 1978.
12. HAURIOU (M-): Precis de droit admmislratif, 12°ed, 1933.
13. High Court London, 24 July 2008, cité dans, Fabrice MATTATIA, Internet et les réseaux sociaux, que dit la loi ? Eyrolles, 2éme edition, 2016.
14. HOLLAND (L-): prscis de droit admmistratif, 9eed, 1953. http://www-rohan.sdsu.edu/~bsavatar/articles/Cyberstalking-NM&S02.pdf.
15. Lagazette.fr :La Police Administrative, Fiche n° 3, publié à l'adresse: https://www.lagazettedescommunes.com/71608/fiche-n%cb0%2-2b-3-la-. LOI 1062-2001 du 15 novembre 2001 relative à la sécurité quotidienne, JORF n°266 du 16 novembre 2001 Texte n° 1;

16. M. CAHEN, Que deviennent les emails, les comptes Webmail et les sites web après un décès? A qui appartiennent – ils ? Rentrent–ils dans la succession?; Paris, 2013, www.murielle–cahen.com.

17. Michele – Laure RASST, Droit pénal special, éd., Dalloz, Paris, 1997.

18. N. TIPPETT, Cyberbullying: Its nature and impact in secondary school pupils. Journal of Child, Psychology and Psychiatry, 2008, N° 49.

19. R. M. KOWALSKI & S. P. LIMBER, Psychological, Physical, and Academic correlates of cyberbullying and traditional bullying, Journal of adolescent health, 2013, n°53.

20. R.Zouaimia, M.–Ch. Rouault, droit administratif, les sources et l'activité l' organization administrative principes généraux administrative – le contrôle de l' administration, BERTI edition, Alger, 2009.

21. Richard STEPPE, The freedom of speech on social networking services, do we need protection against our own expression ?, www.law.kuleuven.be/jura/art/50n3/steppe.pdf.

22. Roger Smith and Alan Paterson: Face to Face Legal Services and Their Alternatives: Global Lessons from the Digital Revolution.

23. Sara Pabian, Heidi Vandebosch, Short–term longitudinal relationships between adolescents (cyber)bullying I perpetration and bonding to school and teachers, International Journal of Behavioral Development, 2016, Vol. 40 (2).

24. Sheryl A. Hemphill, PhD, and others, Predictors of Traditional and Cyber–Bullying Victimization: A Longitudinal Study of Australian Secondary School Students, Journal of Interpersonal Violence, Vol. 30 (15), 2015.

25. Thomas Chevandier et Autres: 50 Questions.. Les polices adminis-tratives, Cahier détachable, No 331, Le Courrier des maires, Février 2019: https://mcit.gov.eg/Upcont/Documents/swf/National_Cybersecurity_Strategy_2023.

26. Tribunal de commerce de Paris, 26 Juillet 2011, cite par: Fabrice MATTATIA, Internet et les réseaux sociaux, que dit la loi ? éd., Eyrolles, 2 éme, Paris, 2016.

سابعًا: المواقع الإلكترونية

1. الموقع الرسمي للجنة الوطنية للمعلوماتية والحريات (CNIL): https://www.legifrance.gouv.fr
2. الموقع الرسمي للجهاز القومي لتنظيم الاتصالات: https://www.tra.gov.eg/ar/.
3. الموقع الرسمي للوكالة الوطنية لأمن نظم المعلومات: https://www.ssi.gouv.fr/.
4. الموقع الرسمي لمقدمي خدمات الاتصال الفوري والاتصال عبر الإنترنت: https://en.arcep.fr/arcep.htm.

قائمة المحتويات

مقدمة.....4
المبحث الأول: مفهوم الضبط الإداري الإلكتروني والتنمر الإلكتروني..... 10
المطلب الأول: مفهوم الضبط الإداري الإلكتروني وهيئاته..... 11
الفرع الأول: مفهوم الضبط الإداري الإلكتروني.....11
الفرع الثاني: هيئات الضبط الإداري الإلكتروني.....23
المطلب الثاني: مفهوم التنمر الإلكتروني وأسبابه وآثاره السلبية.....33
الفرع الأول: مفهوم التنمر الإلكتروني..... 34
الفرع الثاني: أسباب التنمر الإلكتروني وآثاره السلبية..... 49
المبحث الثاني: سلطات الضبط الإداري الإلكتروني في مواجهة التنمر الإلكتروني.....58
المطلب الأول: الإطار التشريعي لمواجهة التنمر الإلكتروني.....59
المطلب الثاني: وسائل الضبط الإداري الإلكتروني في مواجهة التنمر الإلكتروني 79
المطلب الثالث: إجراءات الضبط الإداري الإلكتروني لمواجهة التنمر الإلكتروني..... 101
الفرع الأول: التدابير الوقائية لهيئات الضبط الإداري لمكافحة التنمر الإلكتروني.....102
الفرع الثاني: التدابير العلاجية لهيئات الضبط الإداري لمكافحة التنمر الإلكتروني.....106
الفرع الثالث: الصعوبات التي تواجه هيئات الضبط الإداري الإلكتروني في مواجهة التنمر الإلكتروني وكيفية التغلب عليها.....110
الخاتمة: 115
أولًا: النتائج 115
ثانيًا: التوصيات.....116
قائمة المراجع.....118
قائمة المحتويات.....127