د. ياسر محمد عبد السلام رجب
أستاذ القانون العام المساعد بكلية الحقوق جامعة القاهرة

دور الضبط الإداري الإلكتروني في مواجهة الإنترنت المظلم والإنترنت العميق

(دراسة مقارنة)

المراسلة: د. ياسر محمد عبد السلام رجب –أستاذ القانون العام المساعد، كلية الحقوق، جامعة القاهرة

معرف الوثيقة الرقمي (DOI): https://doi.org/10.54873/jolets.v3i2.155

البريد الإلكتروني: ymar900@gmail.com

نسق توثيق البحث:

ياسر محمد عبد السلام رجب، دور الضبط الإداري الإلكتروني في مواجهة الإنترنت المظلم والإنترنت العميق –دراسة مقارنة، بحث مقدم إلى المؤتمر العلمي الدولي الثالث: الجوانب القانونية للتحول الرقمي «الفرص والتحديات»، كلية القانون بالجامعة البريطانية، الفترة من ١٧–١٨ يونيو ٢٠٢٣، مجلة القانون والتكنولوجيا، المجلد ٣، العدد ٢، أكتوبر ٢٠٢٣، صفحات ٦٥ –١٠٨

دور الضبط الإداري الإلكتروني في مواجهة الإنترنت المظلم والإنترنت العميق (دراسة مقارنة)

د. ياسر محمد عبد السلام رجب

الملخص:

يمتـاز الوضع الـدولي بالتطور التكنولوجي، إلا أن ذلك سرعـان ما أدى إلى ضرورة منحـه الأهمية الكبيرة لمـا يحمله من تأثير كبير على الأنظمـة والمراكز المعلوماتية غير معلومة، فالخطر المعلوماتي خطر جديد يواجه المؤسسات وجهات الإدارة ويكون مرتبطًا بالتطور التكنولوجي، وتدفقات المعلومات.

الأمر الذي أدى إلى ضرورة دراسة أثر الإنترنت في أمن الدول وخصوصاً الجزء المخفي أو المظلـم منه حيث تدار فيه الكثير من العمليـات غير الشرعية أو غير القانونية، وهذا ما جعـل من أمن الدول عرضة للخطر جراء تبنى بعض الجهات لهذه العمليات التي تستهدف الدول، أو الأفراد، أو البنى التقنية الأساسية، أو غيرها من الاعتداءات الإلكترونية.

ويعتـبر الإنترنـت المظلم جـزءاً مهماً من منظومـة الإنترنت؛ حيث يسمـح بإصدار المواقع الإلكترونية ونشر المعلومات بدون الكشف عن هوية الناشر أو موقعه أما الإنترنت العميق هو مجموع كافة المواقع الإلكترونية التي لم تدرج في محركات البحث.

ولمواجهة ما تقدم يعد الأمن السيبراني الحكومي أهم وعاء للأمن السيبراني للدولة ككل نظـرا لتعلقه بالنظام العام، ولذا بناءً على ذلك سوف نبرز في هذا البحث طبيعة الضبـط الإداري الإلكتروني باتصالـه بالفروع المستحدثة قانونيًـا، وغير المطروقة من الفقـه بالفحـص والدراسة كمثال «القانون السيبراني»، أو «قانـون الكمبيوتر»، وكذلك لاتصالـه بقانون التكنولوجيا والمعلومات ومـا يتطلبه مفهوم الضبط الإداري من توسعة لنطاقـه لدرجة تقارب وظيفته مع وظيفة القانون، والدليل أن جهة الإدارة قد تعمد إلى التدخل في الأنشطة والعلاقات الخاصة للأفراد عمليًا لضمان أمنها السيبراني وبحجة الحفاظ على النظام العام.

الكلمات الرئيسية: الإنترنت العميق، أمن الدول الإلكتروني، الأمن السيبراني، شبكة الإنترنت المظلمة، تمويل الإرهاب.

A Comparative Study on the Role of Electronic Administrative Procedures in Combating the Dark Web and the Deep Web

Dr. Yasser Mohammed Abdelsalam Ragab
Associate Professor, Faculty of law, Cairo University

Abstract

The international situation is characterized by technological advancement, but this has soon led to the necessity of giving it great importance due to the significant impact it has on unknown information systems and centers. Information risk is a new threat facing institutions and administrative bodies and is linked to technological development and the plethora of information.

This has led to the necessity of studying the impact of the Internet on the security of countries, especially the hidden or dark part of it, where many illegitimate or illegal operations are conducted, and this is what made the security of countries vulnerable to danger as a result of some parties adopting these operations that target countries, or individuals, Or technical infrastructure, or other electronic attacks

The dark web is considered an important part of the Internet system. It allows the issuance of websites and the dissemination of information without revealing the identity or location of the publisher. The deep internet is the sum of all websites that are not included in search engines.

To confront the above, government cybersecurity is considered the most important container for the cybersecurity of the state as a whole due to its connection to public order. Therefore, based on that, we will highlight in this research the nature of electronic administrative control in its connection with the branches that are legally created and not studied by jurisprudence through examination and study, as an example of «Cyber Law,» or «Computer Law, as well as its connection to technology and information law and the expansion of its scope required by the concept of administrative control to the point where its function is close to that of the law. The evidence is that the administration may deliberately interfere in the activities and private relationships of individuals in practice to ensure their cybersecurity under the pretext of maintaining public order.

Keywords: deep internet, state cybersecurity, cybersecurity, dark web, terrorist financing

المقدمة

أصبحت التكنولوجيا سلاحًا ذا حدين، حيث تعمل التنظيمات الإجرامية على توظيفها في أنشطتها غير المشروعة، وعلى الجانب الآخر تعمل أجهزة إنفاذ القانون على توظيفها في تعقب هذه الأنشطة الإجرامية وضبط مرتكبيها، ومن ثم فإن التكنولوجيا كما يمكن أن تساعد على ارتكاب الجرائم، يمكن أيضًا أن تسهم في مكافحتها، حيث تهيئ الإنترنت فرصًا جديدة لبيع السلع وشرائها بصورة غير مشروعة، سواء عبر الشبكة الواضحة أو الشبكة المظلمة.

وتسعى التنظيمات الإجرامية والإرهابية إلى الاستفادة من مزايا استخدام شبكة الإنترنت المظلمة، وبصفة خاصة طابعها السرى وصعوبة تعقب مستخدميها، بما يحقق لها مباشرة أنشطتها الإجرامية بعيدًا عن أية رقابة أو مساءلة قانونية، وجدير بالذكر أن ممارسة هذه الأنشطة الإجرامية يتطلب ضرورة تضافر جميع الجهود الدولية في مواجهتها، وذلك في ضوء ما يوفره استخدام شبكة الإنترنت من فرص للمجرمين المعلوماتيين من ارتكاب جرائمهم خارج نطاق دولهم، فضلاً عن تسهيلها لعملية التواصل وتبادل المعلومات فيما بينهم، مما يمكنهم من الالتقاء في العالم الافتراضي، والتخطيط والإعداد لارتكاب جرائمهم، والتي يمتد نطاقها إلى أكثر من دولة، وبل في بعض الأحيان قد تستهدف هذه الجماعات الإجرامية المنظمة دولاً أو مؤسسات تجارية أو اقتصادية بعينها، مما قد يؤدى إلى وقوع أضرار اقتصادية جسيمة لهذه الدول أو المؤسسات.

أهداف البحث:

يهدف هذا البحث إلى تسليط الضوء على دور الضبط الإداري الإلكتروني في مواجهة «الإنترنت المظلم والإنترنت العميق ودراسة أثر الإنترنت في أمن الدول وخصوصاً الجزء المخفي أو المظلم منه.

صعوبات وإشكاليات البحث:

تتبلور أبرز صعوبات البحث فيما يتطلبه التعامل مع هذه الشبكة المظلمة من طابع تقني خاص للدخول عليها، ورصد ومتابعة أنشطتها غير المشروعة، نتيجة صعوبة

الوصول إليها من خلال محركات البحث التقليدية، واستخدام تقنيات التشفير المعقدة، التي تعمل على تجهيل هوية مستخدميها وصعوبة التعرف عليهم وتتبعهم، وضبطهم.

منهج البحث:

يعد المنهج الوصفي التحليلي هو أنسب مناهج البحث ، كما أن موضوع البحث وطابعه عبر الوطني يفرض استخدام المنهج المقارن، من خلال الإشارة إلى بعض الوقائع والحوادث ذات الصلة بأنشطة الإجرام المنظم عبر الشبكة المظلمة.

أهمية البحث:

تتبلور أهمية هذا البحث في مجموعة نقاط منها:

١- إن العمليات الإلكترونية انتشرت بشكل واسع، الأمر الذي جعل من الأمن الإلكتروني أهمية رئيسية.

٢- ترتبط أغلب العمليات الإلكترونية في أمن الفرد والذي ينعكس بدوره على أمن الدولة وبهذه الحالة يصبح الأمن الإلكتروني مهمًا لأنه يعرض أمن الأفراد للخطر.

٣- ضرورة تقديم مستوى حقيقي للتهديدات التي يتعرض لها الأمن الإلكتروني لكي ترتقي وسائل المعالجة مع تصاعد حدة الخطورة.

الإشكالية:

الإشكالية هي عما إذا كان الإنترنت العميق ساحة جيدة للاختباء والعمل بسرية عالية وعدم إمكانية ردع واكتشاف مصدر التهديد، ألا يعني ذلك أن الإنترنت العميق أصبح سلاحًا بيد كل من يمتلك القدرة التقنية.

خطة البحث: سوف نتناول البحث في مبحثين:

- **المبحث الأول- محددات الإنترنت العميق والإنترنت المظلم:**
  - المطلب الأول: الإنترنت المظلم والإنترنت العميق (المفهوم والسمات).
  - المطلب الثاني: أثر الإنترنت العميق على أمن الدول.

- **المبحث الثاني: محـددات الضبـط الإداري الإلكتروني لمواجهـة الإنترنت المظلم والإنترنت العميق.**
  - **المطلب الأول:** الجرائم المعلوماتية على ميزان الضبط الإدارى.
  - **المطلب الثاني:** الوسائل التقليدية للإدارة الإلكترونية في مواجهة الجرائم السيبرانية.
  - **المطلب الثالث:** الوسائل الحديثة للإدارة الإلكترونية فى مواجهة المخاطر السيبرانية.

المبحث الأول

محددات الإنترنت المظلم والإنترنت العميق

تجدر دراسة محددات الإنترنت المظلم والإنترنت العميق ضرورة دراسة أثر الإنترنت في أمن الدول حيث تدار فيه الكثير من العمليات غير الشرعية أو غير القانونية، وهذا ما جعل من أمن الدول، عرضة للخطر جراء تبنى بعض الجهات لهذه العمليات التي تستهدف الدول أو الأفراد داخل الدول أو البنى التقنية الأساسية أو غيرها من الاعتداءات الإلكترونية.فبعض التهديدات تؤثر بشكل نفسي واجتماعي و أصبحت العلاقة بين التطور والتهديدات، في المجال الإلكتروني تتناسب طردياً حيث كلما زاد التطور زادت التهديدات وسوف نتناول ذلك المبحث في **مطلبين كالتالي:**

- **المطلب الأول: الإنترنت المظلم والإنترنت العميق (المفهوم والسمات)**
- **المطلب الثاني: أثر الإنترنت العميق على أمن الدول.**

المطلب الأول

الإنترنت المظلم والإنترنت العميق (المفهوم والسمات)

نعيش في عصر الإنترنت والذي من خلاله نقوم بالاتصال مع الأشخاص سوء داخل أو خارج البلاد، ولكن الظاهر لنا من الإنترنت ونستخدمه حتى الآن هو ٥٪ فقط منه بالرغم من كم الرسائل والفيديوهات والمواقع الموجودة أمامنا الآن، ولكن ما يتبقى من الإنترنت هو عبارة عن مكان مظلم لا يمكن الوصول إليه بسهولة، لأنه مباح فيه كل الأفعال المضرة وذلك بسبب أنه لا يوجد أي قوانين تحكمه وهذا المكان اسمه (الإنترنت المظلم).

تحدث مغالطاتٌ كثيرة عند الحديث عن الدارك ويب والديب ويب، حيث يعتقد معظم الناس أن المصطلحين يشيران إلى نفس الموضوع، ولكن هناك اختلافًا هائلًا بين معنى المصطلحين، وما يمثلان من الشبكة العنكبوتية العالمية، **وذلك على النحو التالي:**

وتماشياً مع ما تم ذكره يتألف الدارك ويب (dark web) من مجموعة من المواقع الإلكترونية التي تقوم بإخفاء عنوان الـ IP الخاصة بها، بحيث يحتاج المستخدم

لبرمجيات خاصة للوصول إليها، كما يشكل الدارك ويب نسبةً ضئيلةً جدًا مقارنةً بالديب ويب، ما يقارب (٠,٠١٪) من حجم الشبكة العنكبوتية في العالم.

تتألف شبكة الدارك ويب من عدد قليل جدًا من المواقع الإلكترونية يقدر بالآلاف فقط، وتقوم هذه المواقع باستخدام وسائل وطرق تشفير عديدة، بهدف حجب هوية مالكي الموقع وأماكن تواجدهم.

يشمل الديب ويب جزءًا كبيرًا من الشبكة العنكبوتية العالمية، حيث يشمل جميع المعلومات والمعطيات والمواقع الإلكترونية التي لا يمكن الوصول إليها عن طريق محركات البحث المشهورة مثل جوجل أو بينج، ويطلق على نتائج البحث التي تتمكن محركات البحث من إيجادها بالويب السطحي (surface web)، الذى يشكل ٠,٠٣٪ فقط من المحتوى الموجود على شبكة الإنترنت[١].

علاوة على ما تقدم نشأت بعض الاستخدامات التي تكون في الواقع قانونية لكنها تحتوي على استخدامات وتهديدات للنظام المعلوماتي ولأمن الدول بشكل كبير ومنها الـ(deep Web) والتي تمثل إحدى طبقات الإنترنت، **والتي من الممكن تقسيمها إلى:**

الإنترنت السطحي والذي يشكل ما نسبته ٤٪ تقريبًا من الإنترنت العالمي والذي يتكون من المواقع المتاحة للجميع والتي من الممكن مراقبتها من قبل الجهات الحكومية بكل بساطة.

الإنترنت العميق (deep web) : ويشكل هذا الجزء ٩٦٪ تقريباً من الإنترنت، والذي يكون على مستويات شديدة السرية ولا يمكن مراقبتها وتتبعها نهائيًا من قبل أي جهات حكومية أو غير حكومية واستخدم هذا المصطلح في عام ٢٠٠٩ .

---

(١) د. رامي متولى القاضي : استخدام التنظيمات الإجرامية لشبكات الإنترنت المظلمة. دراسة تحليلية في التشريع المصري https://ncj.journals.ekb.eg/article_225839.html المجلد ٦٤، العدد ٣ – الرقم المسلسل للعدد ٣ نوفمبر ٢٠٢١–المجلة الجنائية القومية، ص ٤٤–١٠٥ .

لا تشكل أغلب مواقع الإنترنت الموجودة ضمن الديب ويب أي مشاكل أمنية على عكس مواقع الدارك ويب، حيث تحتوى المواقع الإلكترونية فيه على محتويات حسابات البريد الإلكتروني المحمي بكلمات سر، بالإضافة للاشتراكات الرقمية في خدمات مثل نيتفلكس وغيرها، ويحمى تواجد هذه المواقع والخدمات مستخدميها من إمكانية الوصول لمحتوياتها عبر عملية البحث البسيطة على أحد محركات البحث ،فلو توفرت هذه المعلومات والمواقع على الويب السطحي أو الـ (surface web)، لتمكن أي شخص من الوصول للرسائل الإلكترونية الخاصة بالمستخدمين بمجرد البحث عنها.

الإنترنت المظلم (dark web): يشتق هذا الجزء من الإنترنت العميق والذي يحتوي علـى عمليات يكون هدفها السرية بشكل أساسـي وبعيدة عن المراقبة والتجسس وغالبًا ما يستخدمها الخارجون عن القانون.

وأول طـرح لهذين المصطلحين جاء في عام ٢٠٠٩ عندما تمت مناقشة مصطلحات البحـث على الشبكة العميقة جنبًا إلى جنب مـع الأنشطة غير القانونية، في حين كانت مقولة «مايكل بيرغمان» عام ٢٠٠١ بأن محركات البحث التقليدية لا تحوي سوى القليل من المعلومات والأكثر يكون في داخلها وبأعماق كبيرة لأن هذه المعلومات تكون غالبيتها مخفية أو مقفلة داخل قواعد البيانات.

وتشير بعض التقديرات الأولية إلى أن الـ (deep Web) يتراوح بين ٤٠٠ و ٥٥٠ مرة أكبر من الشبكة السطحية ومع ذلك فإن الشبكة العميقة تتزايد باطراد بمعدل لا يمكن تحديده كمياً.

وللإنترنت العميق (deepweb) العديد من المستويات التي تتدرج في الخطورة وهي كالتالي:

١- المستـوى الأدنى: يعتبر هذا المستوى هو الأقل خطورة، حيث يحمل بعض البيانات والمعلومات الأكاديمية والحكومية، كما يشتمل على كورسات البرمجة.

٢- المستـوى المتوسط: يضم هذا المستـوى كيفية اختراق الأجهزة والحصول على ما بها من معلومات وصور لابتزاز أصحابها.

٣- المستـوى الأخير: هـو المستوى الأخطر في مستويات (الديـب ويب) والذي يُطلق عليـه (الدارك ويب) وهو يضم العديد مـن الجرائم البشعة والتي قد لا يتخيلها عقل الإنسان، كجرائم الجنس والسرقة والقتل بأبشع الصور الممكنة[١].

أما بالنسبة للإنترنت المظلم فقد تأسس الـ Dark net في التسعينات على يد الجيش

(١) د. رامـي متـولى القاضي : استخدام التنظيمات الإجراميـة لشبكات الإنترنت المظلمة. دراسة تحليليـة في التشريع المصري https://ncj.journals.ekb.eg/article_225839.html المجلـد ٦٤، العـدد ٣ - الرقـم المسلسـل للعـدد ٣ نوفمبر ٢٠٢١-المجلة الجنائية القومية ص ٤٤-١٠٥ .

ومـا يؤخـذ على هذه التقنيات والمتمثلة في الديب ويب، حيث إنهـا تستوعب الكثير من العمليات غير القانونية الإجرامي الذي أدى لـه، فالأمـوال المجنية من النشاطات الخاصة بالجريمـة المنظمة كالاختلاس وتجارة المخـدرات وغيرها عادة ما تتطلب «غسلها» قبل التمكن من استخدامها، والشبكة المظلمة مكان ممتاز لهذه الغاية.

الأمريكي والذي من خلاله يتبادلون المعلومات الاستخباراتية بمنتهى السرية ومن بعدها بدأ الأشخاص المضطهدين والسياسيين يستخدمون الـ Dark net حتى يتحدثوا بحرية من دون معرفة هويتهم [١].

تأكيدًا على ما تقدم يوجد تحت الإنترنت المرئي (Deep Web) والذي يوجد به مواقع لا عدد ولا حدود لها فمن المستحيل رصد هذه المواقع، وهو يوجد به جزء قانوني يضم البيانات التي لا يجب أن تكون متاحة لأي شخص مثل الشبكات الداخلية للمؤسسات التعليمية، أو المؤسسات الحكومية، أو قواعد بيانات الشركات والبيانات التي تحتاج إلى حماية أمنية مثل الحسابات المالية في البنوك، في الوقت نفسه يوجد جزء ليس قانوني مجرد الوصول إليه سوف يوصل بك إلى مواقع القرصنة الإلكترونية مثل موقع Darkode الذي استطاع الـ FBI يقفله سنة ٢٠١٥ وتم القبض على معظم أعضائه في أكثر من ٢٠ دولة.

ويعد ذلك أخطر جزء وهو آخر ٥٪ وهو الـ Dark net الذي يعتبر المأوى لكل الأنشطة غير القانونية، وهو من المستحيل الوصول إليه من خلال محركات البحث العادية، لأن المواقع الموجودة فيه مخفية عن الحركات الموجودة الآن، فإن متصفحات الـ Dark net تستخدم تكنولوجيا onion routing وهذا يوفر للمستخدمين طبقات من الحماية الإلكترونية وتجعل الوصول إليهم ليس سهلاً [٢].

---

(١) د.ذياب البداينة : المرجع السابق، ص ١١٣-١٨١.

هذه الميزة جذبت أشخاص يمارسون أنشطة غير قانونية مثل مواقع تقدم خدمات Hi-t/man يعني أشخاص مجهولين يدفعون أموالاً بهدف قتل أشخاص، بجانب أن انعدام الرقابة يكشف أحقر الجوانب البشرية لدرجة أنه يوجد غرف كاملة في الـ Dark net قائمة على تعذيب البشر مقابل مبالغ مالية عن طريق العملات الرسمية للـ Dark net وهي العملات الرقمية مثل الـ Bitcoin وغيره لأنها ليست تابعة لنظام حكومي فالوصول لمستخدميها أمر صعب جدًا.

(٢) Cairo Time. (٢٠٢٣). إيه هو الدراك من أو الإنترنت المظلم وإيه اللي يحصلك لو دخلت عليه.- https://youtu.be/Pahiy-modj3Q

مجرد استخدامك للـ Dark net يعرضك للمساءلة القانونية لأن في أكتوبر ٢٠٢٠م أعلنت منظمة الأمن العالمية أنها قبضت على ١٥٠ مجرمًا من الـ Dark net في عملية مشتركة ضخمة جدًا سموها Dark HunTOR وتم الوصول في هذه العملية على كمية كبيرة من الأسلحة والمخدرات، وممكن الاطلاع على فيلم Deep Web.

لكن يجب أن نفهم في البداية ما هو الإنترنت تخيل أن هذه الشبكات عبارة عن جبل من الثلج داخل المحيط وله قاعدة داخل المحيط وقمة في الهواء الطلق، وهذا يحدد لنا الـ ٥٪ التي نراهم من الإنترنت ويسمى (الإنترنت المرئي)، وبالرغم من ذلك لكن أن كل ذلك ليس هو الجبل الحقيقي ولكن الجبل الحقيقي يوجد تحت سطح المياه يوجد به كم كبير جدًا من المواقع والمعلومات الغامضة، وهذا يمثل ٩٠٪ من الجبل، وكلما توصلت إلى العمق سوف ترى أخطر جزء من الإنترنت وهو الـ ٥٪ الباقي من هذا الجبل وهذا أخطر مكان في الإنترنت ومن المستحيل الوصول إليه بسهولة وحتى إذا توصلت إليه لا يمكن=

ويرى البعض أن الشبكة المظلمة، لا يمكن الوصول إليها بالطرق العادية، وهي مجال خصب للعديد من الأنشطة الإجرامية غير المشروعة، فليس كل ما هو موجود على شبكة الإنترنت يمكن رؤيته أو الوصول إليه من قبل المستخدمين، فقد ظهر ما يعرف بالشبكات السوداء، والتي يتسم جزء كبير من محتوياتها بطابع السرية، بحيث توفر الخصوصية لمستخدميها بعيداً عن أي نوع من الرقابة، حيث يتم فيها تقديم خدمات وتبادل معلومات بشكل سرى بين أعضائها، ولا يمكن لأى مستخدم خارج الشبكة رؤية محتواها، أو البحث عنها بالطرق التقليدية. وخلاصة القول إن شبكة الإنترنت المظلمة يمكن تعريفها بأنها: جزء من شبكة الإنترنت ، يسمح بإصدار المواقع الإلكترونية ونشر المعلومات بدون الكشف عن هوية الناشر أو موقعه، ويحتاج إلى برمجيات وضبط وتفويض خاص للولوج إليه، وهى جزء من الويب لا تفهرسه محركات البحث، ويمكن الوصول إلى الإنترنت المظلم من خلال خدمات معينة مثل خدمة Tor [1].

ومن جانب آخر، تشير الشبكة السوداء إلى المجتمعات المغلقة على الإنترنت التي يكون الدخول إليها مسموحًا فقط لأعضائها بشكل خاص، ويتم تشفيرها وتشفير المعاملات والأنشطة كافة التي تتم عليها بحيث يستحيل ترقبها، ويتم الدخول عليها من خلال تحميل برامج معينة على جهاز الحاسب الآلي تمكن المستخدم من تبادل كلمات السر مع الأجهزة الأخرى المتصلة على الشبكة نفسها، ويتم نقل المعلومات بين هذه الأجهزة بشكل مشفر تمامًا؛ كالمعاملات البنكية الإلكترونية، وهو ما يجعل الشبكات

= الخروج منه أبدًا، فأنت الآن تتعامل فقط مع ٥٪ من الإنترنت من خلال المواقع .com أو الذي آخرها .org واللي معناها إن هذا الموقع تابع لمؤسسة أو منظمة معينة زي المؤسسات الحكومية، وهذه المواقع يتم الوصول إليها بسهولة.

(١) د. رامي متولى القاضي : المرجع السابق، ص ٤٤-١٠٥.

أولًا- تعريف شبكة الإنترنت المظلمة:

يمكن تقسيم الإنترنت إلى ثلاثة أقسام:

القسم الأول: الشبكة السطحية، التي يتم استخدامها حاليًا، والتي يوجد بها المواقع والمعلومات والبيانات التي يمكن للأفراد الوصول إليها عن طريق محركات البحث التقليدية المتعارف عليها، ولا تمثل سوى (٠,٠٣٪) من المعلومات المتعلقة بها على الإنترنت.

القسم الثاني: الشبكة العميقة، التي تحتوى على قواعد البيانات الأكاديمية والسجلات الحكومية، وقواعد بيانات الشركات والبنوك التجارية، ومحتوى رسائل البريد الإلكتروني وخدمات البث التليفزيوني، والتي تعتبر غير مخالفة للقانون.

القسم الثالث: الشبكة المظلمة.

السـوداء أكثر أماناً من الشبكات الداخلية التي تستخدمها الشركات، والتي لا يتم فيها تشفير الاتصالات بين الأجهزة[١].

خصائص شبكة الإنترنت المظلمة:

تتميز شبكة الإنترنت المظلمة ببعض الخصائص المميزة، من أبرزها:

١- السريـة: تتسم شبكة الدارك ويـب بالسرية التامة التي يتمتـع بها مستخدموها نتيجة التشفير الحاصل لأى بيانات تدخل إليها.

٢- الخصوصية: يحافظ مستخدمو شبكة الدارك ويب على خصوصيتهم بشكل كبير نتيجـة تعطيل أنظمة التشفير المستخدمة ضمنهـا لأى محاولات تعقب إلكترونية لبيانات ومعلومـات المستخدمين، حيث تساعد شبكة التحويلات التي تمر عبرها الإشـارة في حمايـة المستخدم من وصـول معلوماتهم الشخصيـة إلى أصحاب المواقـع الإلكترونية المتواجدة على الدارك ويب، كما يتواجد متصفحٌ يحمل نفس اسـم TOR يستخدم للوصول إليها، بالإضافـة إلى إمكانية استخدامه كمتصفح عادى لباقي أجزاء الشبكة العنكبوتية[٢].

المطلب الثاني

أثر الإنترنت العميق على أمن الدول

يذكـر هـنري كيسنجـر فـي كتابـه النظـام العالمـي أن أشـكال القوة تتغـير بتغير التكنولوجيا وقد أضاف الفضاء الإلكتروني إلى الأشكال التقليدية للقوة معايير جديدة وطـرح مفهومًـا وشكلاً جديداً للقـوة تسمى القوة الإلكترونية وكان لهـذه القوة دور في بلـورة مفهوم انتشـار القوة وتعدد الفاعلـين الممارسين لها سواء من الـدول أو من غير الـدول مما هدد الدور التقليدي للدول وقلل من سيادتهـا على إقليمها ومن خلال ذلك

---

(١) د. رامي متولى القاضي : المرجع السابق ص ٤٤-١٠٥

وعلـى عكـس الشبكة الواضحة التـي تسمى أيضًا «الشبكـة السطحية»، التي تحـول إلى معلومات متاحة للجمهـور وتفهرسها محـركات البحـث التقليدية، فإن الشبكة الخفيـة تتكون من شبكات خفية مشفرة، مما يسمـح لمالك الموقع ومستخدميه على السـواء بإبقاء هويتهم مجهولة مع صعوبـة تعقبها نسبيا، وهو ما يجعلها الشبكة المفضلة لدى كل المجرمين وأصحاب الأنشطة الإجرامية لما توفره من بيئة آمنة لأنشطتهم غير المشروعة التي يرتكبونها بعيدًا عن أيادي سلطات العدالة الجنائية.

(٢) د. رامي متولى القاضي : المرجع السابق ص ٤٤-١٠٥.

يتوفر لمستخدم الإنترنت العميق وخصوصاً الذين يرمون إلى استخدامها لأغراض إجرامية وإرهابية فيتيح لهم الاتصال بمناصريهم وأعوانهم ممن يخشون السلطات في الإنترنت السطحي أو العادي وعلى مستوى مرتفع من السرية بالإضافة إلى جمع المعلومات الكافية التي يحتاجونها في تنفيذ نشاطاتهم في مختلف الجوانب والأماكن الجغرافية.

ومما يؤثر على أمن الدول بواسطة الإنترنت المظلم أو الإنترنت العادي هي الجريمة العابرة للحدود والتي تستهدف نطاق إقليمي أو عالمي وتختلف حسب القائمين بالنشاط الإجرامي من تجارة للمخدرات أو غسيل الأموال أو تبييضها أو كذلك المتاجرة بالأعضاء البشرية أو دعارة الأطفال أو المتاجرة بالأسلحة والتي يكون سببها تنامي الطاقة التكنولوجية للجماعات الإجرامية، بالإضافة إلى ذلك من الممكن أن تشكل كتهديد إلكتروني غير متماثل يعمل على زعزعة أمن الدولة بشكل مستمر خصوصاً في الدول التي تعاني من ضعف التقنية وقلة الخبرة في الجرائم الإلكترونية[1].

علاوة على ما تقدم تشجع السرية والخصوصية العالية لمستخدمي الدارك ويب على القيام بالكثير من الأنشطة غير المشروعة؛ كبيع المخدرات والأسلحة والأجهزة الإلكترونية المسروقة، وتزوير الهويات الشخصية وجوازات السفر، بسبب صعوبة تعقب المستخدمين وكشف هويتهم وأماكن تواجدهم، فأغلب تجارة المخدرات في الوقت الراهن تتم عبر الإنترنت المظلم، وأشهر موقع كان يقوم بهذا هو موقع Silk Road الذى قبضت الشرطة الأمريكية على القائمين عليه عام ٢٠١٣.

توفر بعض مواقع الدارك ويب خدمات لتوظيف مخترقين، ومزورين وحتى قتلة مأجورين، فهناك قتلة مأجورون، يعملون بإرسال صورة الضحية إلى القاتل والاتفاق على سعر معين، وبعد إرسال صورة الضحية مقتولاً يتسلم نقوده من مشترى هذه الخدمة، علاوة على استئجار مخترقي حسابات البنوك والحسابات الشخصية، أو حتى إن أردت سرقة شيء ثمين، فهناك لصوص محترفون يتقاضون أجرًا مقابل عمليات السطو، كما أن هناك مواقع خاصة لبيع المسروقات على الإنترنت .

(١) أمل فوزي أحمد عوض: الحقوق والحريات الرقمية- معالجة قانونية تقنية من منظور الشريعة الإسلامية المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية -يوليو ٢٠٢١ص ٨.

تقـدم الكثير من مواقـع الدارك ويـب خدمات مزيفـةً، بهدف جـذب المستخدمين المبتدئين الذين ليسوا على دِراية كافية بتفاصيل هذه المواقع والخدمات الموجودة فيها، مستغلين الخصوصية والسرية التي يتمتع بها أصحاب المواقع وصعوبة تعقبهم.

يواجـه مستخدمو الدارك ويب خطرًا كبيرًا لإصابـة أجهزة الكمبيوتر الخاصة بهم بواسطة البرمجيات الخبيثة (Malware).

وتـبرز خطـورة استخدام الشبكة المظلمة فـي أنها تشكل بيئة خصبـة وعالمًا خاصًا للمجرمـين المعلوماتيين، لا يخضعون فيه لأى رقابـة (لتعذر وصول السلطات واستحالة تعقبه أو تعقب مستخدميه إذا استعملوه بطريقة صحيحة)، فهو يستخدم كسوق سوداء وكمـكان لتبـادل المعلومـات الممنوعة التي يعاقـب عليها القانون، ومن بـين هذه الأمور: (تعليم صناعة واستخدام الأسلحة والمتفجرات وحتى الأسلحة البيولوجية منها - تعليم الاخـتراق وتبادل البرمجيـات الممنوعة كالفيروسات والثغـرات والتطبيقات الخبيثة - مواقـع بيـع وشراء المخدرات وهى أكـثر ما تنشط التجارة فيها عـبر الإنترنت المظلم- ومواقع مختصة بالتزوير والمعاملات الرسمية المزيفة- مواقع تبادل الكتب والفيديوهات المسروقة[1].

ويثـار التسـاؤل حول استخدام التنظيمـات الإجرامية المنظمـة لشبكة الإنترنت في ارتـكاب جرائمها، حيـث يرى البعض أنه علـى الرغم من أن بعض السمـات التقليدية للجريمـة المنظمـة؛ كاستخدام العنف- علـى سبيل المثال- من الصعـب الأخذ بها في توصيف النشاط الإجرامي السيبراني، إلا إنه ما يستطيع الأفراد فعله، وفى تلك الأسواق

(١) د. رامي متولى القاضي: المرجع السابق ص ٤٤-١٠٥.

ولا تستغرب من وجود مواقع للتواصل الاجتماعي بين مستخدمي هذا الإنترنت، بالإضافة إلى محركات بحث خاصة بالإنترنت العميـق، وقـد ذكر موقـع ويكيبيديا في دراسة أن (٤, ١٥٪) مـن محتوى الإنترنت المظلم يتعلق بالمخـدرات، و(٩٪) للمتاجر الإلكترونية الموجودة فيه، بالإضافة إلى (٦,٢٪) لتبادل ومقايضة العملة الافتراضية المشفرة Bit Coin.

وفـى إنفوجارفيـك نشره مركز المعلومات ودعم اتخاذ القـرار بمجلس الوزراء المصري، تناول فيـه «أسواق الإنترنت المظلمة Dark web marketplaces»؛ أشـار فيـه إلى أن عائـدات التعاملات علـى مواقع الإنترنت المظلم قد شهـدت ارتفاعًا ملحوظًا لتصل إلى ١,٥ مليار دولار وفقًا لآخر بيانات في ٢٠٢٠، مقابل ١,٣ مليار دولار في ٢٠١٩، وأن عمليات الشراء على تلك المواقع تتم عن طريق «العملات المشفرة»، و«البيتكوين» هي العملة الأولى عالميا عليه، وأنه من أبرز أنواع المعاملات على تلك الشبكة: الإتجار بالمخدرات، والأسلحة، وترويج البرمجيات الخبيثة كبرامج الفيروسات، والسلع المزيفة غير الأصلية، وأدوات للجرائم الإلكترونيـة، وأدوات للمراقبـة، كما يوفر أماكن لتخزين البيانات المسروقة، وتتم التعاملات على تلك الشبكة دون الكشف عن هوية أي من أطراف المعاملة، والوسيط هو المسئول عن التسليم، وتظل نقود المشترى تحت تصرفه حتى يتم تأكيد الاستلام.

السـوداء الرقميـة، تُستخدم العملات المشفرة أساسًا لدفع ثمـن المشتريات لتيسير بيع وتداول سلع من قبيل الأسلحة والمخدرات غير المشروعة[١].

تشـير التقديرات إلى أن مثل هذه الأسواق الإجراميـة السيبرانية تضم عددًا كبيرًا من الأفراد، والمنظمات التي قد تكون عابرة، ولاسيما في حالة مهربي الأموال والأعمال والمعامـلات التجاريـة المشبوهة، مثل: استئجـار الروبوتات من فرد واحـد أو مجموعة إلى أخـرى، هذا، وتستخدم شبـكات الروبوت في ارتكاب الهجمات ضد نظم المعلومات وسرقـة البيانات، وتُعرض بتكلفة منخفضة نسبيًا، مستفيدة مـن تقلب حركة الأموال على أساس عدد العملاء[٢]وتحليلًا لبعض الجرائم السيبرانية ذات الدافع المالي، مثل: سرقة بيانات البطاقات المصرفية وبطاقات الائتمان، فقد وجد أن هذه الجرائم ترتكب بأسـواق سوداء من خلال جماعـات وأفراد، يؤدون أدوارًا مختلفـة، ففيهم المبرمجون والموزعـون والخبراء التقنيـون والقراصنة والمحتالون والمستضيفـون والصرافون ونقلة الأموال والزعماء [٣].

(١) د. رامي متولى القاضي : المرجع السابق ص ٤٤-١٠٥.

(٢) د. رامي متولى القاضي : المرجع السابق ص ٤٤-١٠٥.

ومن جانب آخر، تتيح أسواق الشبكة الخفية، التي توصف أيضًا باسم «الأسواق المشفرة، للمشترين والبائعين عدم الكشف عن هويتهم، وتعتبر المنتديات أو غرف الدردشة السرية أحد الأساليب التي تستخدمها الجماعات الإجرامية داخل أسواق الشبكة المظلمـة المسـيرة غالبًا بخدمات إخفاء الهوية، لتبـادل المعلومات والتوسط في بيع الخدمـات الاستشارية، وخدمات الانتشار والفيروس، وتأجير شبكة الروبوت، وخدمات البريد الإلكتروني الطفيلي والاستضافـة وقوائم البريد الإلكتروني والتفاصيل الماليـة، ويضـرب المثـل في ذلك بالمنتديـات التي أنشأها قراصنـة بطاقات الائتمـان لتيسير تبادل بيانـات بطاقات الائتمان المسروقـة، والتي بدأت غالبًا على شكل مجموعات أنشأت على شبكة الإنترنت للالتقاء لتبادل الخبرات وتقديم الخدمات غير المشروعة، ثم بدأت هذه المجموعات في التطور لتتميز بدرجات أعلى من التنظيم الإجرامي.

(٣) د. رامـي متـولى القاضـي : المرجـع السابق صـ ٤٤-١٠٥، علاوة على أن هذه الجماعـات والأفراد تتفاعل مـع عدة عمليات، منها: إعداد البرمجيات الخبيثة، والتحكم في شبكات معلوماتية مصابة من خلال رسائل التصيد الاحتيالي، وإدارة شبكات الروبـوت، والحصـول على البيانات الشخصية والمالية والمتاجرة بالبيانات الماليـة، ومن ثم فإن سوق الجريمة السيبرانية في هذا السياق يمكن تعريفها بأنها «شبكات تواصل اجتماعي تتألف من أفراد ضالعين في نشاط إجرامي منظم»، وليست منشأة مؤلفـة مـن جماعة إجراميه وحيدة، وأنه يمكن التمييز بين طائفتين من الأفراد، الأولى تضم المبرمجين الأصليين للبرمجيات الخبيثـة، وأصحـاب شبكة روبوت قائمة على تكنولوجيـا المعلومات، وهم يمثلون اللاعبين الأساسيـين داخل السوق، والطائفة الثانية تشمل الموزعين المركزيين، وبعض الأفراد الآخرون، والأسراب الذين يحومون حولهم، فمن الواضح أن هؤلاء الضالعين بإعداد وإدارة عناصر السوق الرئيسية، مثل شبكات الروبوت، يباشرون أفعالهم الإجرامية في شكل جماعات صغيرة نسبيًا، أو حتى بشكل منفرد.

المبحث الثاني

محددات الضبط الإداري الإلكتروني لمواجهة الإنترنت المظلم والإنترنت العميق

يعـد الأمن المعلوماتي الحكومي أهم وعـاء للأمن المعلوماتي للدولة ككل نظرًا لتعلقه بالنظـام العام، ولذا تشمل طائفة الجرائم المعلوماتيـة ضد الأمن المعلوماتي الحكومي كل جرائم تعطيل الأعمـال الحكومية وتنفيذ القانون، والإخفاق في الإبلاغ عن جرائم الكمبيوتـر، والحصول علـى معلومات سرية، والإخبار الخاطئ عـن جرائم الكمبيوتر، والعبـث بالأدلة القضائية، وتهديد السلامة العامة، وبث البيانات من مصادر مجهولة، والإرهاب الإلكتروني، والأنشطة الثأرية الإلكترونية أو أنشطة تطبيق القانون بالذات.

وفقًـا لتعزيز الأمـن المعلوماتي يتطلب مفهوم الضبـط الإداري توسعة نطاقه لدرجة تقـارب وظيفته مـع وظيفة القانون، والدليـل أن جهة الإدارة قد تعمـد إلى التدخل في الأنشطـة والعلاقـات الخاصة للأفراد عمليًا لضمان أمنهـا المعلوماتي وبحجة الحفاظ على النظام العام وسوف نتناول ذلك المبحث في مطالب **ثلاثة كالتالي:**

- **المطلب الأول:** الجرائم المعلوماتية على ميزان الضبط الإدارى.
- **المطلب الثاني:** الوسائـل التقليديـة لـلإدارة الإلكترونيـة في مواجهـة الجرائم السيبرانية .
- **المطلب الثالث:** الوسائـل الحديثـة لـلإدارة الإلكترونيـة فـى مواجهـة المخاطر السيبرانية.

المطلب الأول

في الجرائم المعلوماتية على ميزان الضبط الإدارى

تتأتى طبيعة الضبط الإداري الإلكتروني باتصاله بالفروع المستحدثة قانونيًا، وغير المطروقة من الفقه بالفحص والدراسة كمثال «القانون السيبراني»، أو «قانون الكمبيوتر، وكذلك لاتصاله بقانون التكنولوجيا والمعلومات «Information & Technology Law».[١]

وتكمن صعوبة مواجهة الإخلال بالأمن المعلوماتي بسبب خصائص الجرائم المعلوماتية التى تتصف بالعديد من الخصائص التي تجعلها عصية على الضبط الإداري بالمفهوم التقليدي ومن تلك الخصائص **ما يلي:**

١) الطابع الفني الهادئ:

تتصف تلك الجرائم بأنها جرائم فنية يرتكبها شخص ذو خبرة عالية في مجال التقنية المعلوماتية، علاوة على أنها لا تحتاج إلى العنف كالجرائم التقليدية، كما أنها تنطوي على أساليب غير تقليدية؛ لذا يمكن وصفها بالوباء[٢].

٢) الطابع المكاني:

تتصف تلك الجرائم بأنها لا يحدها مكان إذ يمكن لأي شخص بأي مكان أن يرتكب الجريمة في أي مكان آخر، مما قد يثير مشاكل عدة فيما يخص القانون واجب التطبيق علاوة على احتمالية تعارض وظائف الضبط الإداري على الصعيد الدولي.

٣) الطابع الاقتصادي:

علاوة على ما سبق عادة ما تنجم خسائر اقتصادية جراء الجرائم المعلوماتية على الصعيد الحكومي وعلى الصعيد المالي للمؤسسات التجارية والاقتصادية خاصة إذا أخذنا في الاعتبار تدني نسبة الإبلاغ عن تلك الجرائم لعدم زعزعة ثقة العملاء.

---

(١) يتصل ذلك المفهوم بالفضاء السيبراني (CYPER SPACE) أو الفضاء التخيلي ويرجع الفضل في ذلك المصطلح للمؤلف وليام جبسون ليشير به إلى الحقيقة التخيلية لشبكات الكمبيوتر، وقد تفرع عن ذلك المصطلحات الآتية:-
Cyper «Cyper cash – Cyper time – Cyper crime»
وغيرها من التعبيرات التي تنطلق في فكرة البيئة التخيلية أو الافتراضية . للمزيد انظر.. منير محمد الجنبيهي، ممدوح محمد الجنبيهي ،المرجع السابق ص٧٥، ٧٦.

(٢) د/ ذياب البداينة: الأمن وحرب المعلومات، دار الشروق للنشر والتوزيع، الأردن ٢٠٠٢ ص١٠٣ .

وفـي اعتقادنا أن نتائج الجريمـة المعلوماتية قد تؤدي للتأثير على سمعة الدولة على المستويـين المحلي والدولي، حيث قد ترتكب تلك الجرائم بدافع الرغبة في قهر النظام السياسي ، وإحراج جهة الإدارة أكثر من شهوة الحصول على الربح المادي[١].

مـن جماع ما سبق يعد الأمن المعلوماتي الحكومي أهم وعاء للأمن المعلوماتي للدولة ككل نظـرًا لتعلقـه بالنظام العـام؛ ولذا تشمل طائفـة الجرائم المعلوماتيـة ضد الأمن المعلوماتي الحكومي كل جرائم تعطيل الأعمال الحكومية وتنفيذ القانون، والإخفاق في الإبـلاغ عن جرائـم الكمبيوتر، والحصول على معلومات سريـة، والإخبار الخاطئ عن جرائم الكمبيوتر، والعبث بالأدلة القضائية، وتهديد السلامة العامة، وبث البيانات من مصـادر مجهولة، والإرهاب الإلكتروني، والأنشطة التأرية الإلكترونية أو أنشطة تطبيق القانون بالذات[٢].

وهنـاك العديد من المخاطـر الأخرى التي تهدد الأمـن المعلوماتي لجهة الإدارة كالتالي:

١) **اخـتراق النظـم:** ويكون ذلك عـن طريق دخول شخص غير مخـول له بالدخول حتى وإن لم يؤثر ذلك سلبيًا على النظام.

٢) **زراعـة نظـم الضعف:** ويكون ذلك باستخدام الشخـص غير المخول له بالدخول باستخـدام النظام بـزرع مدخل ما يمكنه من اختراق النظام ومن أمثلة ذلك (فيروس حصان طروادة).

٣) **مراقبـة الاتصال:** ويكون ذلك عـن طريق مراجعة إحدى نقـاط الاتصال بدون اختراق الحواسب الآلية.

٤) **اعتراض الاتصالات.**

(١) مثـال ذلك مـا تعرضت له امتحانـات الثانوية العامة في مصر من تسريبـات هددت سير العملية التعليميـة، وأخلت بمفهوم النظـام العـام.، حيث يميـل مرتكبو هذه الجرائم إلى إظهار تفوقهـم ومستوى براعتهم، وتزداد الدوافـع لدى الشباب الذين يحاولون كسر حواجز الأمن لأنظمة الحاسب الآلي وشبكات المعلومات».

(٢) د/ أيمن عبد الله فكري، المرجع السابق، ص١٠٠.

٥) إنكار الخدمة[١].

ويقع دور الحكومة في حرب المعلومات الدفاعية في عدة مناطق هي: الدفاع الوطني، وتأسيس الحمايات القانونية، وإرساء المقاييس، والبحث والتطوير من تقنيات جديدة للدفاع ففي الولايات المتحدة الأمريكية يتمتع مكتب التحقيقات الفدرالية بصلاحيات التحقيق في التجاوزات التي تحدث على القانون الفدرالي، وبالقيام بأعمال مضادة للتجسس وبتنسيق مثل هذه الأعمال في الولايات المتحدة الأمريكية[٢].

لذا تعمل الحكومات على حماية البنية التحتية الحيوية، وتشمل تلك البنية المعلومات والاتصالات والبنوك والماء والصحة العامة وخدمات الطوارئ، والطاقة، والنقل، والصناعات الكيماوية، والمواد الخطرة[٣].

ويثور التساؤل عن صور الإخلال بالأمن المعلوماتي لجهة الإدارة بصورة خاصة.

في الواقع يمثل القرصان الإلكتروني السياسي (أو مخترق المعلومات ذات الطابع

---

(١) محمد محمد صالح الألفي، المرجع السابق، ص ١٢٠.

للمزيد انظر:

– محمود الرشيدي: الجرائم الإلكترونية والتأمين الإلكتروني، «قضايا المركز الدولي للدراسات المستقبلية والاستراتيجية العدد ١١ السنة الأولى، نوفمبر ٢٠٠٥، ص٣٠-٣٢.

وكذلك محمد أمين الرومي: جرائم الكمبيوتر والإنترنت – دار المطبوعات الجامعية، الإسكندرية ٢٠٠٤.

(٢) د.ذياب البداينة : المرجع السابق، ص ١١٣-١٨١.

(٣) «ومن أوائل الدول التي عملت على هذا النحو في التشريعات العربية الإمارات العربية المتحدة، حيث جاء القانون الاتحادي الإماراتي لسنة ٢٠٠٦ بوجوب الحفاظ على بيانات الحكومة الاتحادية والحكومات المحلية».

يقصد بالبيانات الحكومية في المادة الأولى من القانون الاتحادي الإماراتي: البيانات الحكومية الاتحادية وبيانات الحكومات المحلية والهيئات والمؤسسات العامة الاتحادية والمحلية، بل عمد المشرع في المادة(٢٢)من القانون إلى توسعة مفهوم البيانات الحكومية بأنها تشمل الدخول بدون وجه حق إلى موقع أو نظام معلوماتي بقصد الحصول على بيانات أو معلومات سرية، والمتتبع لمسارات التجريم في ذلك القانون عند تعلق الأمر بالأمن المعلوماتي لجهة الإدارة يجد التجريم التالي:

– تجريم إيقاف أو تعطيل الشبكة أو تدمير وحذف البيانات (المادة ٦ من القانون).

– التدخل في القطاع الطبي بإتلاف الفحوصات الطبية (المادة ٧ من القانون).

– إعاقة الوصول لبيانات ومعلومات الشبكة المعلوماتية (المادة ٥ من القانون).

– الإضرار بالنظام العام الأخلاقي الآداب العامة (المادة ١٢ من القانون).

– الإضرار بالأمن العام عن طريق ترويج المخدرات والمؤثرات الفعلية (مادة ١٨ من القانون).

– الإضرار بالنظام العام والآداب العامة عن طريق ترويج أفكار وبرامج معينة (مادة ٢٠ من القانون).

– الإضرار بالنظام العام عن طريق الإرهاب الإلكتروني (م ٢١ من القانون).

السياسي) أخطـر أنواع المخترقين الإلكترونيين الذين يهـددون الأمن المعلوماتي لجهة الإدارة والأمثلة الإلكترونية على ذلك عديدة[١].

ومـن أمثلة مخترقي المعلومات السياسيـة دوليًا ما أعلنته وزارة العدل الأمريكية من إدانـة خمسة ضباط اشتركوا في عملية سرقة معلومات وبيانات سرية تخص مجموعة من الشركات الأمريكية[٢].

وعلى الصعيد المقابل ألقت الإدارة الأمريكية بتهمة الهجوم الإلكتروني على شركات صينية لشبكات الهواتف النقالة بغرض سرقة ملايين الرسائل النصية[٣].

ولا يقتصـر الأمر على مجال التجارة والاتصالات، بـل امتد ليشمل الإخلال بالأمن العام بصفة خاصة وتهديد النظام العام المادي بصفة عامة[٤].

علاوة على ماسبق يرى الفقه المقارن أن من أخطر أنواع الهاكرز الذين ينتهكون الأمن المعلوماتي لجهة الإدارة هو النوع الذي يقوم بسرقة المعلومات الحساسة (التجسس).

Net spoinage (theft of confidential information)

فرغـم تعدد أنـواع القراصنة الإلكترونيين[٥] إلا أن ذلك النـوع إلى جانب القرصان

---

(1) Steven Philippsohn, Trends in cyber crime - An overview of current financial crimes on the internet, computers & security, 20 (2001) p. 54.

تم استغـلال الهجمـات الإلكترونية داخل إطار الخلافـات السياسية كمثال الأزمة بـين كوسوفو وصربيا، واكتشـاف اليابان وجود هجمات كيميائية من جماعة AUM على محطات المترو هناك، وكذلك الهجمات على مواقع مثال Yahoo، CNN، Amazon، ZD، eBay وكلها مواقع تجارية شهيرة لذا عمد الرئيس الأمريكي «كلينتون» وقتها لاعتماد ٢ بليون دولار أمريكي لتعزيز الأمن المعلوماتي الأمريكي.

(٢) مروان صالح، المرجع السابق ص١٥.«وطالت تلك الهجمات عددًا من مقاولي الدفاع والأمم المتحدة، واللجنة الأولمبية الدولية فـي منتصف عام ٢٠٠٦، بل وطالـت الهجمات بيانات مهولة، كمثال سرقة مخططات التصنيـع، ونتائج الاختبارات، وخطط العمل، ووثائق التسعير، واتفاقات الشراكة، ورسائل البريد الإلكتروني، وقوائم الاتصال»

(٣) المرجع السابق، ص١٦، «نقلا عن تسريبات إدوارد سنودن مسئول الأنظمة السابق لوكالة الاستخبارات الأمريكية «CIA» حيث قرر أن وكالة الأمن القومي «NSA» تستهدف الشبكات الرئيسية «Network Backbones».

(٤) فـي عـام ٢٠١١ ظهر الجيش السوري الإلكتروني SEA والذي قام بتخريـب العديد من المواقع عن طريق البرمجيات الخبيثة، ويبـدو أن تلـك الخلية الإلكترونية لها تسلسل هرمي واضح المعالم، يتكون من قـادة وخبراء تقنيين، وأذرع إعلامية ومئات من المتطوعين، ينتمي العديد منهم إلى الجمعية العلمية السورية المعلوماتية، حيث كانوا يعملون بنظام القرصنة الجماعية المنظمة حكوميًا.

(5) Steven Phillippsohn, op. cit., p. 55, 56
«The types of criminal Hackers are:-
1) Hackers A) External Hacker.
B) Hacking to highlight lack of security.

الإلكـتروني السياسـي والقرصان الإلكـتروني الإرهابي يمثلون أخطر أنـواع القراصنة الذين يهددون الأمن المعلوماتي لجهة الإدارة.

حيـث يعمل ذلـك النوع الأول من القرصنـة على سرقة المعلومـات الحساسة وبيعها لمـن يقوم بالدفع بأعلى سعـر ويطلق عليه القرصان المتجسـس Net spoinage theft of confidential information)) وقد واجهت الجهة الإدارية في الصين ذلك[١].

أما النوع الثاني وهو الإرهاب الإلكتروني أو السيبراني (cyber – terrorism) يتزايد خطره من خلال الأسلحة الإلكترونية على جهة الإدارة والتي تتمثل في القنابل المنطقية logic bombs والقنابـل الكهربائية المغناطيسيـة eletromagnetic bombs، والتي تتاح لـدى العصابـات الإلكترونية، والتي يمكنهـا أن تعطل الأجهـزة والمراسلات الحكومية وغيرها إذا لم يتحقق تهديدها وابتزازها للمؤسسات أو الهيئات الخاصة والعامة[٢].

٤) الطابع المتصل بالأمن القومي:

كمـا ذكرنـا سلفًـا تتصـل الجرائـم المعلوماتيـة بالطابع الأمنـي القومـي والطابع

2) Internet Hackers.
3) Internet Saboteur.
4) Net spoinage (theft of condifential Information).
5) E. Theft.
6) Credit Card fraud.
7) Pump & Dump.
8) Cyber Terrorism.
9) Cybor privacy.
10) Virus.
11) Fraudulent internet Banking sites.

(١) قامـت الجهـة الإداريـة في الصـين بغلق ١٢٧ مقهى إنترنـت لقيامها بنشر أسـرار الدولة وبث العديد مـن المعلومات شديدة السرية.

وبمتابعـة المواقع الإخبارية والإلكترونية فى ٢٢مايو ٢٠١٧ نجد وجود صدى واسع لهجوم «الفدية الخبيثة» الإلكترونى المعروف باسـم «WannaCry» وهـو آخر تجليات برمجيات الابتزاز الإلكترونى والذى أصاب ربع مليون مستخدم للدولة فى حوالى ١٥٠ دولـة حول العالم مابين الغاء عمليـات جراحية،واختراق مواقع إلكترونية جامعية، وتعطيل محطات القطارات فى ألمانيا،وقدر خـبراء صناعة الإنترنت الفدية المدفوعة للقراصنة بمبلغ٢٠ألـف دولار تم دفعها من خلال «عملة البيكوتين» التى لايمكن تتبع مصدرها.

(2) Ibid, p. 60

ويشـير الكاتـب هنا أن العصابـات الإلكترونية تبيع تلـك الأسلحة كمثال العصابـات الروسية وتقوم تلـك العصابات بإبتزاز المؤسسـات العامة والخاصة وتهديدها إن لم تقم بدفع مبلغ مـالي مقابل عدم استخدام تلك الأسلحة الإلكترونية، وأبرز مثال لذلـك عندمـا تم استهـداف الكمبيوتر الرئيسي لبنـك اليابان، ولكن تم إخطـار FBI في الوقت المناسـب وتم إفشال الهجوم بسرعـة، لكن في أغلب الأحيان تفشل المؤسسات فـي إخطار السلطات المختصة، ومثال ذلك: قيام بيت السمسرة البريطاني بدفع فدية قدرها ١٠ مليون جنيه استرليني وقيام البنك البريطاني بدفع ١٢,٥ مليون جنيه استرليني بعد تهديدات.

السياسي، ونجد ذلك فيما يعرف بحرب المعلومات والتجسس الإلكتروني، والإرهاب الإلكتروني[١].

وعادة ما تلجأ الدول تحت الهاجس الأمنى القومى إلى كبت الحريات وإلى وضع قيود إضافية على استخدام الإنترنت، كالقانون الذي أصدرته تركيا، والذي يمنح هيئة الاتصالات التركية الصلاحية والترخيص بإغلاق مواقع الإنترنت في خلال أربع ساعات، ولكن المحكمة الدستورية العليا التركية اشترطت استصدارحكم قضائي قبل إغلاق أي موقع، ورأت المحكمة عدم دستورية النص الذي يتيح للهيئة الحصول على معلومات من خلال رقابتها لبعض المواقع عبر مستخدميه ثم تخزينها[٢].

ويرى الفقه المقارن أنه ولكون مصطلح «الأمن القومي» مصطلحًا سياسيًا فإنه من المرونة ما يؤثر على حرية التعبير وتداول المعلومات؛ ولذلك فإنه مصطلح مجرد وغامض ويفترض أن يكون محدد المعنى كي يوازن بين حق المواطن في المعرفة، ومصلحة الإدارة في الحفاظ على الأمن المعلوماتي[٣].

وعلى صعيد الواقع العملي تميل الجهات الإدارية لتفضيل كفة الحفاظ على الأمن القومي، وذلك لتفضيل الحكومة بالمفهوم السياسي الابتعاد عن النقد فيما يخص تصرفاتها وأعمالها، ويتجسد ذلك التفضيل في حجب المعلومات التي تتعلق بعملية صناعة القرارات، أو النشاطات غير المشروعة، أو الفساد.

وعامة يعد الأمن القومي للدولة هدفًا رئيسيًا قبل وجود الدولة ذاتها، ويعد شرطًا لاحقًا لأنشطتها بعد ذلك؛ لذا من المقبول أن تتبع الإدارة العديد من الإجراءات السرية فيما يخص معاملاتها[٤].

---

(١) مشار لتلك الأمثلة في مؤلف د/ حسين الغافري، المرجع السابق، ص١٥ نقلاً عن:

- د/ منصور محمد عقيل ود/ على قاسم، الإنترنت والأبعاد الأمنية، مركز البحوث والدراسات الشرطية، دبي، يناير ١٩٩٦، ص١٢-١٣. «ومثال ذلك: سرقة معلومات عسكرية من أنظمة الحاسبات الآلية الخاصة بسلاح البحرية الفرنسية في صيف ١٩٩٤، ومثال ذلك أيضًا: ما تعرضت له عدة وزارات وجهات حكومية ومؤسسات مالية من هجوم من جماعات الألوية الحمراء عن طريق تدمير مراكز المعلومات الخاصة»

(٢) جريدة الأهرام المصرية الورقية - العدد اليومي بتاريخ ٥ أكتوبر ٢٠١٤.

(3) Shimon shetreet: free speech and national security, International studies in Human Rights - Volume 16 p. 44.
«The notion of national security is so abstract and vague that it must be given specific content»
«Right of the public to know, and the Interest of keeping certain Matters secret».

(4) Ibid, p. 59.

ولكـن من غير المقبول أن يتسع النشـاط السري في أنشطة جهة الإدارة سواء زمنيًا أو موضوعيًا بشكل مطلق، بل يعد ذلك محكومًا بأن تعالج السرية بأدوات ضرورية فقط تحـدد ذلك الهدف[١]، وتتبايـن تلك المفاهيم من دولة إلى أخرى بحسب طبيعة النظام السياسي، وفي ذات البلد من وقت لآخر.

ومـن أهم تلك المفاهيم «مفهوم الأمـن القومي» حيث يعد مفهومًا متلازمًا مع الأمن المعلوماتـي، وقـد عرف القانون رقـم ١٥ لسنة ٢٠٠٣ بتنظيم الاتصـالات مفهوم الأمن القومـي فـي المـادة الأولى منـه[٢] كما تم تعريـف أجهزة الأمـن القومي بأنهـا رئاسة الجمهورية ووزارة الداخلية، وهيئة الأمن القومي، وهيئة الرقابة الإدارية ويذهب بعض الباحثين إلى أن ذلك التعريف جاء عامًا شاملاً لكل ما يتعلق بأنشطة تلك الأجهزة[٣].

وتجـدر الإشـارة إلى أن الاعتماد بشكل كامـل على التقنيـات الإلكترونية في حفظ الأمـن المعلوماتي قد يضر بالأمن القومـي، إذ ستكون المعلومات معرضة لتصرف الغير في حين لا تكون التقنيات تحت السيطرة من كل جوانبها، علاوة على ذلك تواجه الدول الناميـة معضلة الفجوة الرقميـة، والتي تمثل الحد الفاصل بين مـن يملكون وتتاح لهم التقنيـات المعلوماتية، وبين الذين لا يتاح لهم ذلك، وعادة ما تكون الفجوة أكثر وضوحًا وأوسع في الدول النامية، نتيجة العوائق التعليمية والاقتصادية والتنظيمية[٤].

ومـن أبرز ما يهـدد الأمن القومى مـا يعرف بالإرهـاب الإلكتروني وهـو استخدام الفضاء الإلكتروني cyper space كأداة لإلحاق الضرر بالبنى التحتية الحرجة كالطاقة، والمواصلات، وعمليات الإدارة أو تعطيلها[٥].

ويؤثـر الإرهاب الإلكتروني على نطاقات الأمـن المعلوماتى من خلال قيام المنظمات المتطرفـة بالإخـلال بالنظام العام وخاصـة فى عنصر الأمن العـام وعن طريق تهديد

(1) Ibid, p. 59 «The secrecy is instrumentally necessary for the promotion of a goal».

(٢) نصـت المـادة الأولى بند ٢٠ من القانون على أن مفهـوم الأمن القومي يشمل كل ما يتعلق بشئـون رئاسة الجمهورية، والقوات المسلحـة والإنتاج الحربي ووزارة الداخلية، والأمن العام، وهيئة الأمـن القومي، وهيئة الرقابة الإدارية والأجهزة التابعة لهذه الجهات يعد من أجهزة الأمن القومي.

(٣) أحمد عزت وآخرون: حرية الفكر والتعبير – الطبعة الثانية ٢٠١٣ ، ص٦٠.

(٤) د/ نبيل علي، د/ نادية حجازي: الفجوة الرقمية – رؤية عربية لمجتمع المعرفة، عالم المعرفة – الكون – أغسطس العدد (٣١٨) ٢٠٠٥ ، ص٧ مشار إليه لدى د/ عبد السلام هابس السويفان، المرجع السابق، ص١٠٩، ١١٠.

(٥) د/ عادل صادق: استخدام الإرهاب الإلكتروني في الصراع الدولي – دار الكتاب الحديث بدون سنة نشر. ص١٠٥ .

الفضاء المعلوماتي من أجل أغراض سياسية أو بدوافع دينية من خلال تكنولوجيا الاتصال والمعلومات والهواتف المحمولة والحاسبات الآلية وعبر شبكة الإنترنت[١].

وقد عرفت وكالة المخابرات المركزية الأمريكية مصطلح الإرهاب الإلكتروني بأنه هجوم تحضيري ذو دوافع سياسية موجه ضد نظم معلومات الكمبيوتر وبرامجه.

أما مركز حماية البنية التحتية القومية الأمريكية فقد ذهب إلى أن الإرهاب الإلكتروني عمل إجرائي يتم تحضيره عن طريق أجهزة الكمبيوتر والاتصالات السلكية واللاسلكية ينتج عنه تدمير أو تعطيل الخدمات بهدف إرباك وزرع الشك بهدف التأثير على الحكومة أو السكان[٢].

والتعريف الذي يؤيده الفقه هو: «العدوان أو التخويف أو التهديد ماديًّا أو معنويًّا باستخدام الوسائل الإلكترونية الصادر من دول أو جماعات أو أفراد عبر الفضاء الإلكتروني، أو أن يكون الفضاء الإلكتروني هدفًا لذلك العدوان بما يؤثر على الاستخدام السلمي له»[٣].

وما نميل إليه هو أن الإرهاب الإلكتروني صورة للإخلال بالنظام العام في أى عنصر من عناصره من خلال نشاط أو هجوم متعمد بغرض التأثير على القرارات الحكومية أو الرأي العام أو من خلال التأثير المعنوي والنفسي عبر التحريض على بث خطابات الكراهية الدينية وحرب الأفكار، أو أن يتم في صورة رقمية للإضرار بالأمن المعلوماتي للأفراد أو المؤسسات أو الدولة ككل[٤].

لذا فإن حرب الشبكات تشير إلى الصراعات التي تقودها المعلومات، وهي تعني

---

(١) من أمثلة ذلك: تطوير تنظيم القاعدة برنامجًا أطلق عليه (أسرار المجاهدين ٢) وهو أول برنامج للتراسل الآمن في ذلك الإطار عبر الشبكات وكان يعد ذلك فى حينها أعلى مستوى تقني في التراسل المشفر (المرجع السابق ص١١٧).

(٢) مشار لتلك التعريفات في مؤلف د/ عادل صادق – المرجع السابق، ص١٠٦.

(٣) المرجع السابق، ص١٠٩.

(٤) نستبعد من ذلك التعريف باستخدام الأسلحة التقليدية كالقصف المباشر القذائف على نقاط الإنترنت الرئيسية ومهاجمة كابلات الاتصال أو القيام بهجوم عن طريق استخدام الطاقة الكهرومغناطيسية للقيام بهجوم إلكتروني Electronic Attack ضد أجهزة الكمبيوتر والبيانات بداخلها رغم أنها داخلة في تعريف الإرهاب الإلكتروني ولكنها ترتبط بالقانون الدولي العام بصورة أوضح.

ويرى د/ عادل صادق أن هجمات الفضاء الإلكتروني تؤثر على الأمن والطابع المدني له والدليل على ذلك الحرب الجورجية الروسية عام ٢٠٠٨ والحرب الروسية الآستونية عام ٢٠٠٧.

التركيـز على آراء النخبـة أو آراء الجماهير أو هما معًا، ومن أبـرز أنواع تلك الحروب التسلـل إلى شبكات الكمبيوتر وقواعد البيانات لتخريبهـا، ومحاولة تدعيم الجماعات المنشقة أو المعارضة في بلد ما من خلال شبكات الكمبيوتر. وبالتالي فإن حرب الشبكات تتميز باستهدافها للمعلومات والاتصالات[١].

وعلـى الرغـم من هذه الجهـود لمجابهة صـور الإجرام عـبر الشبكـة المظلمة، فإن هنـاك بعض الأصوات التـي تؤيد استخدام الشبكات المظلمـة وبرنامج TOR والبرامج المثيلـة له، نظـرًا لاستخدامهم كأدوات للتعبير عن الـرأي وحماية خصوصية المواطنين في مواجهـة الرقابة الحكومية، علاوة علـى التوقعات المستقبليـة لاستخدام الشبكات السـوداء والمواقـع والتطبيقـات المنبثقة عنها فـي إحداث تغييرات جذريـة في النظام العالمـي وفواعله، وبصفة خاصة العملات الافتراضيـة، والتي يتصاعد استخدامها في المجتمعات الافتراضية[٢].

المطلب الثاني

الوسائل التقليدية للإدارة الإلكترونية في مواجهة الجرائم السيبرانية

ستكون معالجة هذا المطلب كالتالي:

أولاً- الضبط فى المدلول اللغوى:

للضبـط لغة عدة مفاهيم، فهو يعنى أولاً دقة التحديد فيقال ضبط الأمر بمعنى أنه حـدد علـى وجه الدقة، وهو يعنـى ثانيًا وقوع العينين ثم إلقـاء اليدين على شخص كان خافيًـا ويجرى البحث عنه، والمعنى الثالث يفهم منه العود بالأمور إلى وضعها الطبيعى المنسجـم مـع القانون الحاكم لهـا وذلك عقب خلـل أو اضطراب أصابهـا منحرفًا بها عـن حكم هذا القانون[٣]، ويقال أيضًا فـى تعريف الضبط لغة، ضبط (ضبط) الشىء

(١) السيـد ياسين: شبكـة الحضارة المعرفية من المجتمع الواقعي إلى العالم الافتراضي – الهيئـة المصرية العامة للكتاب، سلسلة العلوم الاجتماعية ، ٢٠٠٩، ص١٠٣.

(٢) د بشيخ محمد حسين – المراقبة الرقمية: الضبط الإداري في مواجهة منطق الإنترنت– مراقبة الإنترنت وأثرها على الحريات العامة –المكتب العربي للمعارف الطبعة الأولى ٢٠١٩ من صفحة ٢١٨ إلى ٢٨٩١.

(٣) انظر الدكتور رمسيس بهنام: علم النفس القضائى، الإسكندرية، منشأة المعارف، سنة النشر غير مذكورة، ص١٥.

حفظـه بالحزم وبابـه ضبط ورجل (ضابـط) أى حازم[١]، ويقال أيضـاً الضبط لزوم الشىء وحبسه لا يفارقه فى كل شىء[٢].

ثانياً- الضبط فى المدلول الاصطلاحى:

(١) تعريف الفقه العربى للضبط الإدارى:

تباينـت وجهات النظر بشـأن تحديد ماهية الضبـط الإدارى وتعريفه، فذهب البعض إلى أن الضبط الإدارى مهمته وقائية، تنحصر فى المحافظة على النظام العام، والحيلولة دون وقوع الجرائم، ومن ثم يعرف بأنه، حق الإدارة فى أن تفرض على الأفراد قيـودًا تحد بهـا من حرياتهم بقصـد حماية النظام العـام[٣]. ولذا يعـرف هذا الرأى الضبـط الإدارى بأنه «مجموعة مـا تفرضه السلطة العامة من أوامـر ونواه وتوجيهات ملزمة للأفـراد بغرض تنظيم حرياتهم العامة، أو بمناسبـة ممارستهم لنشاط معين، بهدف صيانة النظام العام فى المجتمع»[٤].

ويرى البعض أن وظيفة الضبط الإدارى تعتبر وظيفة تتسم بخصائص متميزة، فهى ضروريـة ومحايدة وهادفـة إلى وقاية النظام العام فى المجتمع فـى ظل سيادة القانون وبوسائل السلطة العامة[٥].

ويعرف البعض الضبـط الإدارى بأنه «النشاط الذى تتولاه الهيئات الإدارية، ويتمثل فى تحديد النشاط الخاص بهدف صيانة النظام العام»[٦].

ويـرى البعض فـى تعريفه للضبـط الإدارى ضـرورة التركيز على الهـدف منه وهو صيانـة النظام العام دون اشـتراط أن يكون الإجراء الضبطى ماسًّا بالحريات، لأنه قد

---

(١) قاموس مختار الصحاح، الطبعة الثالثة، ص٤٠٠.

(٢) قاموس لسان العرب، الجزء التاسع، القاهرة، الدار المصرية للتأليف والترجمة، ص٢١٤ فصل الضاد، حرف الطاء.

(٣) انظـر الدكتـور سليمان محمد الطماوى: الوجيـز فى القانون الإدارى «دراسـة مقارنة»، القاهرة، دار الفكـر العربى، ١٩٧٩، ص٥٧٤.

(٤) انظـر الدكتـور طعيمة الجرف: القانـون الإدارى والمبادئ العامة فى تنظيم ونشاط السلطـات الإدارية، القاهرة، دار النهضة العربية، ١٩٧٨، ص٤٨٧.

(٥) انظـر الدكتـور محمـود سعد الدين الشريف: النظريـة العامة للضبـط الإدارى، مقالة منشورة بمجلة مجلـس الدولة، السنة الحادية عشرة، ١٩٦٢، ص١١٢.

(٦) انظر الدكتور محمود عاطف البنا: الوسيط فى القانون الإدارى، القاهرة، دار الفكر العربى، ١٩٨٤، ص٣٣٧.

لا يمس إلا مجرد رخص، فيعرف الضبط الإدارى تبعًا لذلك بأنه «مجموع الأنشطة التى تتخذها الإدارة منفردة بهدف المحافظة على النظام العام أو إعادة هذا النظام فى حالة اضطرابه»[١].

وذهب البعض إلى أن وظيفة السلطة التنفيذية هى السهر على تنفيذ القوانين، ولا يقتصر ذلك على المعنى الحرفى للتنفيذ، بل يتناول أيضاً وقاية وحماية النظام الاجتماعى، فالسلطة التنفيذية لها بحكم وظيفتها ما يشبه التفويض العام فى المحافظة على النظام العام[٢].

(٢) تعريف الفقه الفرنسى للضبط الإدارى:

ومن أقدم التعريفات فى الفقه الفرنسى تعريف الفقيه «NICOLAS. DELAMARE» الذى حدد أغراض الضبط فى أحد عشر جزءًا يشملها النظام العام وهى «الدين، النظام، الآداب، الصحة، الأغذية، الأمن، السكينة العامة، الطرق، العلوم والفنون الحرة، التجارة، الصناعات والفنون الميكانيكية، المرافق المحلية، العمال غير المختصين (عمال اليومية) والفقراء[٣].

أيضاً وفى نطاق هذا الاتجاه لتعريف الضبط الإدارى يقرر الفقيه «CLAUDEKLEIN» أن السمة المميزة للضبط الإدارى هى جاهزيته «ADAPTABILITE» وقابليته للتكيف، وتلك الجاهزية تأتى من طابعه الغائى، حيث يرى أن سلطة الضبط مادامت مكلفة بحفظ النظام فإنها تتهيأ وتتكيف مع كل أسباب الاضطراب المستقبلى للنظام العام مهما كان الشكل الذى يتخذه[٤]. وفى اعتقادنا أن ذلك التعريف أكثر تواؤماً مع التطور الحالى للجرائم المستحدثة والطفرة الكبيرة فى الجرائم المعلوماتية.

هذا ويعرف البعض الضبط الإدارى تعريفًا موسعًا فيعرفه PAPANICOLAIDIS بأنه «مجموع النشاطات القمعية والمادية التى تقوم بها السلطات الإدارية سواء لضمان

---

(١) انظر الدكتورة سعاد الشرقاوى: القانون الإدارى، القاهرة، دار النهضة العربية، ١٩٨٣، ص١٢.

(٢) انظر الدكتور محمد أنس قاسم جعفر: الوسيط فى القانون العام «أسس وأصول القانون الإدارى»، دار النشر غير مذكورة، سنة النشر غير مذكورة، ص١٦٣.

(3) «La religion, la discipline, les moeurs, la sante, les vivres, la surete et la tranquillite publique, la voirie, les sciences et les arts liberaux, le commerce, les manufactures et les arts mecaniques, les servitudes domestiques, les manoeuvriers et les pauvres».

(4) KLEIN (C.) : «La police du domaine public», Paris, L.G.D.J., 3e ed, 1966, p. 37.

حسـن النظام فى المجتمع أو داخل المرافق العامة، أم لحماية السلامة المادية للأملاك العامة»[١].

هـذا ويـرى BLAEVOET أن غرض الضبـط سلبـى تمامـا حيـث إن شعـاره لا اضطرابـات، ولذلك يعرف الضبـط الإدارى فيقول «إن الضبط نظام موضوعة تدارك أى إخـلال محـدق بالنظام العـام، أو بوقفـه إن كان قد وقع، ولكن فقـط إذا كانت قد تعرضت لـه الأماكن العامة أو تلك التى يرتادها الجمهور والأحوال الطبيعية الخارجية للوجـود»[٢]. وفى اعتقادنـا أن ذلك التعريـف لا يتواءم مع الجرائـم المستحدثة عامة، والجرائم المعلوماتية خاصة إذ أن الإدارة لا يكون موقفها سلبياً على الدوام، بل لابد أن تأخذ بعنصر المبادرة دوماً كى تحفظ الأمن المعلوماتى.

ثالثًا- الحدود المتعلقة بوسـائل الضبط الإدارى فى الظروف العادية والظروف غير العادية:

يتعين فـى وسائل الضبط الإدارى لكى تكون فى إطار الشرعية القانونية وهى تواجه ممارسـة الحريـة، أن تقوم علـى عدة محـاور يكمل بعضهـا البعض تتطلبهـا ضرورة صيرورتهـا مشروعـة، ويمكن إجمـال أهم هـذه الضوابط التى يمكـن استخدامها فى مواجهة الجرائم المستحدثة **كالتالى:**

- أن يكون التدبير الضابط ضروريًّا ولازمًا وفعالاً.
- أن يكـون التدبير الضابط متناسبًا مع طبيعة وجسامة الخلل والاضطراب المراد تفاديه.
- أن يكون التدبير الضابط متصفًا بالعمومية محققًا للمساواة.

(١) أن يكون التدبير الضابط ضروريًّا ولازمًا وفعالاً لمواجهة الجريمة المستحدثة:

يشـترط فى التدبـير الضابط أن يكون ضروريًّا ولازمًا بمعنـى أن تكون غايته تفادى خطـر حقيقى يهـدد النظـام العام، فالخطـر البسيط الذى قـد يلحق بالنظـام العام لا يرخص للإدارة مشروعية اتخاذ التدبير الضابط.

(1) PAPANICOLAIDIS (D.) : introduction generale a la theorie de la police administrative, Th, Paris, 1958, L.G.D.J., ed. 1960, pp. 15-16.
(2) BLAEVOET (C.) : des recours juridictionnels contre les mesures de police, Th, Paris, 1908, pp. 14-15.

وتقـدر الضرورة بقدر جسامة التهديد الذى يخشـى منه على النظام العام، وهو ما يستوجب أن يكون التدبير المتخذ من قبل الإدارة لازمًا لتوقى الخطر دون أى تدبير آخر أقـل منه إعاقة للحريـة، وبالتالى فليس من المقبول أن تكون وطأة التدبير الضابط أشد وطأة من ذات الشدة التى يراد اتقاؤها.

ولقد أرسى المجلس مبادئ هذه الرقابة فى حكمه الشهير فى دعوى «BENJAMIN» بتاريخ ١٩٣٣/٥/١٩، فقـد أصدر عمدة «NEVERS» قرارًا بمنع عقد أحد الاجتماعات خشيـة من وقـوع اضطرابات تخل بالنظام العام، ولقد ألغـى مجلس الدولة هذا القرار بعد فحص الظروف التى أحاطت بالدعوى إلى الاجتماع[١].

أيضاً فقد أخذت المحكمة الإدارية العليا بتلك القاعدة، حيث قضت فى أحد أحكامها «بأنـه لإيقـاف إدارة أحـد المحـال الصناعية والتجاريـة باعتباره من المحـلات المقلقة للراحة والمضرة بالصحة والخطرة، أو إلغاء رخصته فإنه يشترط أن يكون هناك خطر داهم يتعذر تداركه، غير أن ذلك الإيقاف أو الإلغاء منوط بوجوب ثبوت الحالة الواقعية المبررة للتدخل بإجراءات الضبط الإدارى ثبوتًا مقنعًا فى جدية الإجراء ولزومه.

(٢) أن يكـون التدبيـر متناسـبًا مع طبيعة وجسـامة الخلل والاضطـراب المراد تفاديه:

يشـترط فى التدبير الضابـط أن يكون متناسبًا مع مدى جسامـة الاضطراب الذى تهدف الإدارة إلى تفاديه، فإذا كان الاضطراب قليل الأهمية فلا يجب أن تكون التضحية بكامل الحرية أو تقييدها فى المجال الأكبر لها، ويستلزم ذلك ضرورة النظر إلى منزلة الحرية التى يراد المساس بها لاتقاء الخطر.

وتأسيسـاً علـى ما تقدم، فقد قضـى مجلس الدولة الفرنسى بإلغـاء تدابير الضبط التـى تتضمن قسوة شديدة فى تقييد الحريات إذا كان يكفى لتحقيق مقتضيات النظام أن تتخذ الإدارة من جانبها بعض الاحتياطات التقليدية[٢].

أيضـاً تراقب المحكمة الإداريـة العليا ملاءمة تلك الإجـراءات، فمن ذلك ما قضت بـه من أنه «فيمـا يتعلق بالحريات وجـب أن يكون تدخل الإدارة لأسبـاب جدية تبرره.

(1) E.E. 5 Mars 1978, Jeunesses indep chretiennes, D., 1949. J. 1947.
(2) C.E. 26 Octobre 1928, S., 1929. 3. 61.

فالمنـاط، والحالة هذه، فى مشروعيـة القرار الذى تتخذه الإدارة هو أن يكون التصرف لازمـاً لمواجهة حـالات معينة من دفع خطر جسيـم يهدد الأمن والنظـام، باعتبار هذا الإجـراء الوسيلـة الوحيدة لمنع هـذا الضرر، وللقضـاء الإدارى حـق الرقابة على قيام هـذا المسوغ أو عدم قيامه، فإذا ثبت جديـة الأسباب التى تبرر هذا التدخل كان القرار بمنجاة من أى طعن. أما إذا اتضح أن الأسباب لم تكن جدية ولم يكن فيها من الأهمية الحقيقية ما يسوغ التدخل لتقييد الحريات كان القرار باطلاً[1].

(٣) أن يكون التدبير الضابط متصفًا بالعمومية محققًا للمساواة:

تخضع الحريات العامة والحقوق لمبدأ أساسى وجوهرى هو مبدأ المساواة، ومفاده أن الأفراد متساوون فى الحريات والحقوق لا تفرقة بينهم فى ذلك لأى سبب من الأسباب.

تأسيسـاً علـى ما تقدم، يتعين فى التدبـير الضابط أن يكون متصفًـا بالعمومية فى مواجهـة الأفراد، فهـذه الصفة تستهدف تحقيـق المساواة بين الأفـراد المتصلين بهذا التدبـير والمستهدفـين منه، فتمنع وبذلك التمييز بين حالـة مشابهة وأخرى مما تدخل فـى مجـال تطبيقه، ومن ثم تعتبر ضربًا من ضروب تحقيـق الضمانات للحرية بوصف كونهـا تمثـل قيدًا على سلطة الضبـط عند ممارسة نشاطها بتدابيرهـا الضبطية على اختلاف أنواعها.

ويثـور تساؤل فى سياق مختلف وهو هل تحتاج مواجهة الجرائم المستحدثة فى إطار الأمن المعلوماتى للضبط الإدارى فى حالات الظروف الاستثنائية.

فـى الواقع توجد العديد من النصوص الدستورية والقوانـين الاستثنائية أو كليهما معـا والتى تمنح لجهـات الضبط السلطات التي تمكنها من التصـرف لإبعاد الأخطار، وإلى جانب تلك النصوص والقوانين ابتدع القضاء نظريات مكملة للنصوص – الحلول القضائيـة للظـروف الاستثنائية – تضفـي المشروعية على بعض أعمـال الضبط التي تتخذ لمواجهة تلك الظروف.

ولا تعنى الحلول التشريعية والقضائية للظروف الاستثنائية أن تتحلل هيئات الضبط مـن الخضوع لمبدأ المشروعية فى هذه الظـروف، إذ أن هذا المبدأ يجب أن يكون موضع

(١) انظـر حكم المحكمة الإدارية العليا فى القضية ١٥١٧ لسنة ٢ق، والصادر بجلسة ١٣/٤/١٩٥٧، منشور بمجموعة المبادئ التى قررتها المحكمة الإدارية العليا للسنة الثانية تحت رقم ٩٣، ص٨٨٦.

احترامها فى الظروف العادية والاستثنائية على حد سواء.

تتطلب الظروف الاستثنائية – على ما سبق أن أوضحناه – الترخيص للإدارة بممارسة السلطات الاستثنائية، حتى ولو خالفت مبدأ المشروعية، مع ما يرتبه ذلك من تقييد للحريات الفردية، فالضرورات الحيوية للبلاد ومصالح الدفاع القومى والأمن العام، أى الدفاع عن الدولة، تكون أولى بالرعاية من احترام حقوق وحريات الأفراد، ففى الأوقات العادية تكون الحريات الشخصية فى الاعتبار الأول، أما فى الظروف الاستثنائية، فإنها تخلى مكان الصدارة لمقتضيات الدفاع عن الدولة[1]. وفى اعتقادنا أن التوازن بين الحقوق الفردية والأمن القومى المعلوماتى لابد أن يكون هدفاً للإدارة فى الظروف العادية ولكن فى الظروف غير العادية لا بد من وضع الأمن المعلوماتى على موقع الصدارة.

ولقد عبر عن المعانى السابقة مجلس الدولة الفرنسى فى حكمه الشهير «DOLET LAURENT»، فقد قرر بأنه «لا تستوى القيود المفروضة على سلطات الضبط الإدارى فى وقت السلم ووقت الحرب، فمصالح الأمن القومى زمن الحرب توسع من مفهوم ومتطلبات النظام العام، كما تبرر إجراءات ضبط إدارى أكثر شدة»[2].

وقد عمد مجلس الدولة فى أحكامه إلى توضيح القيود والضوابط التى ينبغى أن تلتزمها الإدارة فى هذا الصدد، وفى هذا تقول المحكمة الإدارية العليا «إن قضاء هذا المجلس ثبت منذ إنشائه على أن نظام الأحكام العرفية فى مصر وإن كان نظامًا استثنائيًا إلا أنه ليس بالنظام المطلق، بل هو نظام خاضع للقانون أرسى الدستور أساسه وأبان القانون أصوله وأحكامه ورسم حدوده وضوابطه، فوجب أن يكون إجراؤه على مقتضى هذه الأصول والأحكام وفى نطاق تلك الحدود والضوابط، وإلا كان ما يتخذ من التدابير والإجراءات مجاوزًا هذه الحدود أو منحرفًا عنها عملاً مخالفًا للقانون تنبسط عليه الرقابة القضائية إلغاءً وتعويضًا. فكل نظام أرسى الدستور أساسه ووضع القانون قواعده هو نظام يخضع بطبيعته – مهما كان نظامًا استثنائيًا – لمبدأ سيادة القانون ومن ثم لرقابة القضاء».

(1) Note HAURIOU sous C.E. 28 Juin 1918, Heyries; Rec 651, cite in, S., 1922.3.49.
(2) C.E. 28 Fevr 1919, Dames Dol et Laurent, Rec 208, S., 1918-1919.3.33.

المطلب الثالث

الوسائل الحديثة للإدارة الإلكترونية فى مواجهة المخاطر السيبرانية

هنــاك العديد من الوسائل الحديثة التى على الإدارة الإلكترونية أن تتغياها للوصول إلى مواجهة شاملة للجرائم السيبرانية ومنها:

أولاً- تأمين الشبكات على نحو يمنع من اختراقها:

لعل فــى محاولة الشركات والمؤسسات الخاصة والحكوميــة تأمين شبكاتها الخاصة بالكومبيوتر ضد الاختراق بمثابة وسيلة تحد – إن لم تمنع مطلقاً – من عملية الاختراق لهذه الشبكات، ومن ثم فهى تؤدى بطريقة غير مباشرة إلى منع الأحداث من الانحراف الإنترنتى بطريق اختراق هذه الشبكات.

وجدران النار عبارة عن برامج تقوم بصد محاولات الاختراق أو الهجوم الوافد من شبكة إنترنت لتهديد الشبكة الداخلية أو النظام المعلوماتى، وتوجد برامج كثيرة لجدران النار من ذلك برنامج شبكة (DAN) والذى يتضمن مزايا أمنية عديدة عبارة عن برامج جدران النار Firewalls، ومزودات بروكسى Proxy servers التى تحتفظ بصفحات الشبكة – للويب – على القرص الصلب، ومرشحات عناوين arl filters.

ومن طرق تحصين الشبكات الداخلية كذلك من الاختراق عملية التشفير، والتشفير يعنــى تحويــل البيانات المكتوبة إلى أرقــام أو رموز لا يمكن حلهــا إلا بالنسبة لمن يمتلك شفــرة حل هذه الرموز والأرقام، وتستخدم عمليــة التشفير فى تداول النقود والبيانات عبر الشبكة فى التجارة الإليكترونية، وفى تداول غيرها من البيانات التى تتعلق بالأمن القومى، وهناك برامج تشفــير متقدمة لحماية البيانات المخزنة على شبكات الحاسب الآلى.

ثانيـاً- تأهيل رجال الضبط والتحقيق الجنائـى والمحاكمة فى مكافحة جرائم الإنترنت:

فـى مكافحة جرائم الإنترنت بصفة عامة، وجرائم الأحداث بسبب الإنترنت بصفة خاصة لا بد من وضع سياسة جنائية رشيدة تستند إلى تدريب أجهزة العدالة الجنائية للأحداث، لمكافحة الجريمة، بما فيها الجريمة المعلوماتية، ويمتد التدريب إلى العاملين فـى الشرطة أو فى القضاء أو فى التنفيذ، وقد تنبهـت الدول إلى أهمية هذا التدريب، وظهـر هذا الاهتمام فى توصيات العديد مـن المؤتمرات الدولية الخاصة بمنع الجريمة ومعاملـة المجرمـين، منها ما جاء فى القاعدة (٢٢-١) مـن (قواعد بكين) من التأكيد علـى الحاجة إلى التخصصـ المهنى والتدريب وورد فيها أنـه «يستخدم التعليم المهنى والتدريب أثناء الخدمـة ودورات تجديد المعلومات وغيرها من أساليب التعليم المناسبة مـن أجـل تحقيق واستمرار الكفـاءة المهنية اللازمـة لجميع الموظفين الذيـن يتناولون قضايا الأحداث».

ولهـذا يجب إعداد المحققـين ورجال الضبط فى جرائم الحاسـب الآلى والإنترنت، لأنهم يواجهون أنشطة إجرامية معقدة وتنفذ بطريقة دقيقة وذكية من الكبار والأحداث على حد سواء.

وليـس بالضـرورة أن يكون المحقق خبيراً فى الحاسـب الآلى، لكن لابد له من الإلمام ببعض المسائـل الأوليـة التـى تمكنه مـن التفاهـم مع خـبراء الحاسـب الآلى وحسن استغلالهم فى كشف الجرائم وجمع الأدلة، كما أنه من الضرورى أن يكون المحقق ملمًّا بالإجراءات الاحتياطية التـى ينبغى اتخاذها على مسرح الجريمة فى جرائم الحاسب الآلى، والتدابير اللازمة لتأمين الأدلة ومعلوماتها المغنطة بصورة علمية وسليمة[١].

وإذا كانـت الشـركات الخاصـة تستعـين بمحققين هـم خبراء فـى الحاسب الآلى، فالجهـات الحكوميـة أولى بإعـداد كوادرها للضبـط والتحقيق فى جرائـم المعلوماتية والإنترنت [٢].

(١) راجع د/ محمد الأمين البشرى فى «التحقيق فى جرائم الحاسب الآلى» بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت. مقدم إلى كلية الشريعة والقانون – جامعة الإمارات العربية المتحدة – الفترة من ١-٣ مايو ٢٠٠٠م.

(٢) فالتقـدم المتواصـل فى تكنولوجيا الحاسب الآلى والإنترنت، يفترض أن جهات تطبيق القانون يجب عليها أن تسير فى خطوات متناسقة مع التطورات السريعة التى تشهدها هذه التقنيات، وهذا الأمر يتطلب الإلمام بالتقنيات الجديدة حتى يمكن مواجهة=

ويتعين ملاحظة أنه ليس من المطلوب أن ينفرد رجل الضبط القضائى أو خبير الحاسب الآلى بتحقيق الجريمة المعلوماتية كاملة، لكن كلاهما يكمل دوره، دور الآخر، فكل منهما له خبرات ومعارف يجب أن تسخر لمصلحة التحقيق فى مثل هذه الجرائم، وهناك محققون متمرسون فى جرائم الحاسب الآلى، ولم تكن دراستهم الأولى فى هذا المجال، وهناك مجموعة من صغار المحققين لديهم الإلمام بعلوم الحاسب الآلى، الأمر الذى يقتضى التعاون بين هؤلاء لمصلحة العمل، عن طريق تبادل المعرفة والخبرة بأسلوب علمى.

وقد كان هناك من يرى أن صعوبة التحقيق الجنائى فى جرائم المعلوماتية يتطلب منا أن نعهد بتحقيق هذه الجرائم إلى بيوت خبرة متخصصة فى هذا المجال، خاصة وأن هناك شركات عالمية حققت نجاحاً فى بعض الحالات.

ويجب أن تشمل خطة التدريب والتأهيل أولئك القائمين على جمع الاستدلالات والتحقيق الابتدائى والحكم فى هذه الجرائم، ويتعلق منهج التدريب والتأهيل كذلك بتدريس الأساليب الفنية المستخدمة فى ارتكاب الجريمة، أو الأساليب التى تتعلق بالكشف عنها والجرائم والأدلة المستخدمة فى ارتكاب هذه الجرائم وكيفية إثباتها ومعاينتها والتحفظ عليها، وكيفية فحصها فنياً وتدريب القضاة على معالجة هذا النوع من القضايا التى تحتاج إلى خبرات عالية، وذلك حتى يمكن قبول الأدلة الناشئة عنها فى الإثبات وتقديرها، وحتى يمكنهم فى النهاية الفصل – بجدارة – فى هذا النوع من الجرائم[١].

وينظم البوليس الدولى كذلك دورات تدريبية فى مجال شبكات الحاسبات الآلية من أجل تحسين أداء الأعضاء من رجال الضبط القضائى فى مجال الكشف عن الجريمة وجمع المعلومات ومتابعة الجناة وإقامة الدليل فى الجرائم التى ترتكب فى هذا المجال[٢].

= مجرمى المعلوماتية. وهذا الأمر واضح فى مؤسسات القطاع الخاص، نظراً للأجور العالية التى يقبل هذا القطاع أن يدفعها لهم، فهناك تعاون بين العاملين فى تطبيق القانون والخبراء المتخصصين فى نطاق القطاع الخاص.

من ناحية أخرى فإن إعمال القانون فى مواجهة جرائم المعلوماتية تستلزم اتخاذ إجراءات قد تتجاوز المفاهيم والمبادئ المستقرة فى قانون العقوبات التقليدى.

راجع: بيتر إن جرابسكى – الجريمة فى فضاء الإنترنت – ص٧٧.

(١) د/ جميل عبد الباقى الصغير – أدلة الإثبات الجنائى والتكنولوجيا الحديثة – دار النهضة العربية – القاهرة – ٢٠٠١، ص١١٨.

(٢) د/ جميل عبد الباقى الصغير – أدلة الإثبات الجنائى والتكنولوجيا الحديثة – مرجع سابق – ص١١٨.

وأما عن الإجراءات التى يجب مراعاتها من قبيل الخبراء الفنيين عند جمع الاستدلالات فى جريمة معلوماتية **فتخلص فى الآتى:**

١- تحديد نوع نظام المعالجة الآلية للمعلومات، وهل هو كومبيوتر معزول أو متصل بشبكة.

٢- وضع مخطط تفصيلى للمنشأة التى وقعت بها الجريمة مع كشف تفصيلى عن المسئولين بها ودور كل منهم.

٣- إذا وقعت الجريمة على شبكة، فيجب حصر طرفيات الاتصال بها أو منها.

٤- مراعاة صعوبة بقاء الدليل فترة طويلة فى الجريمة المعلوماتية.

٥- مراعاة أن الجانى قد يتدخل من خلال الشبكة لإتلاف كل المعلومات المخزنة.

٦- إبعاد الموظفين عن أجهزة الحاسب الآلى، بعد الحصول منهم على كلمات السر Passwords وكذلك الشفرات فى حال وجودها.

٧- تصويب الأجهزة المستهدفة التى وقعت بها أو عليها الجريمة[1].

ثالثًا- تأمين بيانات الحكومة الإلكترونية فنياً:

وتخلص وسائل الحماية الفنية لبيانات الحكومة الإلكترونية فى الآتى:

١- الجدار النارى أو حوائط المنع Fire Walls:

الجدار النارى عبارة عن مجموعة أنظمة معلوماتية – برامج توفر سياجات أمنية ما بين شبكة إنترنت وشبكة المؤسسة – أو الحكومة الإليكترونية – حتى يتم إجبار جميع عمليات الخروج من الشبكة والدخول إليها، بأن تمر من خلال هذا الجدار النارى، والذي يمنع أى مخترق أو متطفل من الوصول إلى الشبكة.

٢- مكافحة الفيروس المعلوماتى:

يعرف الفيروس المعلوماتى بأنه «برنامج للحاسب الآلى مثل أى برنامج آخر، لكنه يهدف إلى إحداث أكبر ضرر بنظام الحاسب الآلى، وله القدرة على ربط نفسه بالبرامج

(1) Dogin, Henry S., Computer crime: Criminal justice resource manual Washington. D.C.U.S. Government printing office, 1996, p. 68.

الأخرى، وكذلك إعادة إنشاء نفسه حتى يبدو كأنه يتكاثر ويتوالد ذاتياً، ويقوم الفيروس بالانتشار بين برامج الحاسب الآلى المختلفة، وبين مواقع مختلفة فى الذاكرة»[١].

ومشكلة الفيروس المعلوماتى هوقدرته على الاختفاء والقدرة على الانتشار والتدمير، وتتم مواجهته ببرامج حماية (anti-virus).

٣- وسائل أخرى:

العبور، وهناك التوقيع الإلكترونى، وهناك شهادات التصديق على هذا التوقيع الإلكترونى، وكذلك تقنية التشفير الذى يرد على بيانات ومعلومات الحكومة الإلكترونية، وكلها برامج معلوماتية تساعد فى حماية نظام وبيانات الحكومة الإلكترونية.

(١) د/ عبادة أحمد عبادة – التدمير المتعمد لأنظمة المعلومات الإلكترونية – بحث منشور لدى مركز البحوث والدراسات، الإدارة العامة لشرطة دبى – مارس ١٩٩٩.

وكذلك د/ هدى قشقوش – جرائم الحاسب الآلى فى التشريع المقارن – دار النهضة العربية – القاهرة – ١٩٩٢، ص٩٩.

الخاتمة

الخطـر المعلوماتى خطـر جديد يواجـه المؤسسات وجهـات الإدارة ويكـون مرتبطًا بالتطـور التكنولوجـي، وتدفقات المعلومات ويمكن تعريفه بأنـه تهديد إلكتروني محتمل يتعلـق بالمعلومـات والبيانات الرسميـة وغير الرسميـة للمؤسسات والأفـراد والجهات الإدارية والحكومية.

الأمـر الذي دعى إلى ضرورة دراسة أثـر الإنترنت في أمن الدول وخصوصاً الجزء المخفي أو المظلم منه حيث تدار فيه الكثير من العمليات غير الشرعية أو غير القانونية، وهـذا ما جعل من أمـن الدول عرضة للخطر جراء تبنى بعض الجهات لهذه العمليات التـي تستهـدف الدول أو الأفراد داخـل الدول أو البنى التقنيـة الأساسية أو غيرها من الاعتداءات الإلكترونية.

يعد التطور التكنولوجي العامل الأساسي في تغير شكل التفاعلات الدولية من خلال التأثـير المتزايـد على الفواعل داخل هـذه التفاعلات فأصبح الفرد فاعـلاً في النظام الـدولي من خلال ما يمتلكه من تقنية عالية مؤثرة في الأمن الدولي من خلال امتلاكه أو انضمامه إلى جماعات الإرهاب الإلكتروني.

وكانـت الساحة المناسبة لهذه الطاقات والمكانيات الإلكترونية الإنترنت العميق الذي تتم فيه عمليات مخالفة للقانون بشكل سري وبدرجات عالية من الخطورة والتعقيد.

وبعـد توضيـح مفهوم ومستويـات وسمات الإنترنـت العميق الأمر الـذي أدى نتيجة التطـور المعرفي إلى اتساع التهديدات الإلكترونية والـذي أدى تلقائيًا إلى زيادة أثارها وخطورتها بالإضافة إلى أثر الإنترنت العميق في أمن الدول، الأمر الذي جعلنا نستنتج مجموعة من النتائج متمثلة في **الاتي:**

١- إن الإنترنـت العميق يعمل في مجال تقني خاص به بعيد عن كل حالات المراقبة والمتابعة.

٢- إن الأفـراد يلجـأون إلى هـذا الإنترنت لأنه يتيح لهـم إمكانيـة التخفي والقيام بالأعمال التي تدر عليهم مكاسب قد تكون مالية أو انتقامية أو غيرها من الدوافع الأخرى.

٣- يتضمن الإنترنت العميق حالات كثيرة من الجرائم والتهديدات الإلكترونية التي تهدد أمن الفرد والدولة انتقال جزء من أنشطة الجماعات الإجرامية المنظمة إلى الواقع الافتراضي، مستغلين الشبكة المظلمة كسوق سوداء وبيئة خصبة لمباشرة أنشطتهم الإجرامية، وتشير التقديرات إلى تحقيق هذه الجماعات المنظمة لأرباح ضخمة من هذه الأنشطة غير المشروعة، معتمدين في ذلك على العملات الافتراضية المشفرة.

٤- نتيجة التطور التكنولوجي أصبحت العلاقة بين التطور والتهديدات في المجال الإلكتروني تتناسب طردياً حيث كلما زاد التطور زادت التهديدات.

٥- يعرض الإنترنت العميق أمن الدول للخطر المادي والمعنوي فبعض التهديدات تؤثر بشكل نفسي واجتماعي، خاصة فيما يتعلق باستغلال المجرمين المعلوماتيين ما تتسم به الشبكة المظلمة من سرية واستخدام تقنيات التشفير المعقدة التي تصعب عملية متابعتهم وتعقبهم، لمباشرة أنشطتهم الإجرامية، بعيدًا عن نظر سلطات العدالة الجنائية، بما يشكل عائقًا في ملاحقة هذه العناصر الإجرامية، وصعوبة إثبات الجرائم المرتكبة.

التوصيات:

١- نقترح أن تعمل السلطات التنفيذية على توفير متطلبات الضبط الإداري الإلكتروني من خلال تهيئة أدوات البيئة المعلوماتية الآمنة، وأولها الإدارة الإلكترونية، والحكومة الإلكترونية.

٢- نقترح أن تعمل الجهات الإدارية على وضع سياسة أمنية معلوماتية عامة للمواطن العادي، وسياسة أمنية معلوماتية أكثر خصوصية للموظف العام لكون الأمن المعلوماتي الحكومي الأكثر تطلبًا، والأكثر حساسية.

٣- نقترح أن تعمل الجهات الإدارية على وضع إدارات أو وحدات إدارية خاصة بنظم المعلومات وأمنها بكل هيكل تنظيمي للوزرات والإدارات الحكومية وغيرها.

٤- نوصي الإدارات العامة المصرية بالولوج إلى الآليات المستحدثة من نظام الإدارة الإلكترونية ومحاولة الاستفادة منها في تطوير أعماله وترسيخ أمنها المعلوماتي، خاصة مع تعقد آليات الضبط الإداري على الصعيدين العملي والقانوني.

٥- ضرورة تضافر الجهود الدولية وتعزيز التعاون الدولي الأمني والقضائي، لتحقيق المواجهة الفعالة لمواجهة أنشطة الإجرام المنظم عبر الشبكة المظلمة.

٦- النظر نحو استحداث وحدات أمنية متخصصة لمكافحة جرائم الشبكة المظلمة والعملات المشفرة، وتعزيز دور منظمة الإنتربول في التنسيق بين هذه الوحدات، لتحقيق المواجهة الفعالة في مكافحتها.

٧- العمل على دعم أجهزة إنفاذ القانون بالمساعدات التقنية والتدريب المتقدم اللازم لإجراء أعمال التحري المتعلقة بالشبكة الخفية وكيفية ضبط الجرائم المرتكبة عبر الشبكة المظلمة.

٨- مواصلة العمل على تطوير الحلول التقنية المساعدة لرصد وكشف الجرائم المرتكبة على الشبكة المظلمة كأدوات التنقيب على المعلومات والزواحف الشبكية لفهرسة البيانات على الشبكة المظلمة والأدوات التحليلية لتعقب مسارات العملات الافتراضية المشفرة وبرمجيات سلاسل الكتل للتحفظ على الأدلة الرقمية.

المراجع

أولاً- باللغة العربية:

الكتب:

- **د. أحمد محمد مرجان:** دور الإدارة العامة الإلكترونية والإدارة المحلية في الارتقاء بالخدمات الجماهيرية- دراسة مقارنة بين الإدارة المحلية في مصر وبلدية دبي في دولة الإمارات العربية المتحدة، الطبعة الثانية، دار النهضة العربية القاهرة، ٢٠١٠م.
- **بروفيسور أورين كير وبيتر إن جرابسكى:** الجريمة فى فضاء الإنترنت.
- **د. جميل عبد الباقى الصغير:** أدلة الإثبات الجنائى والتكنولوجيا الحديثة – دار النهضة العربية – القاهرة – ٢٠٠١.
- **د. خالد سمارة الزعبي:** القانون الإداري وتطبيقاته في المملكة الأردنية الهاشمية، الطبعة الثانية، مكتبة دار الثقافة للنشر والتوزيع- عمان، ١٩٩٣.
- **د. رمزي طه الشاعر:** قضاء التعويض – مسئولية الإدارة عن أعمالها غير التعاقدية، «دون طبعة»، دار النهضة العربية، القاهرة، ١٩٨٦م.
- **د. رمسيس بهنام:** علم النفس القضائى، الإسكندرية، منشأة المعارف بدون سنة نشر.
- **د/ رمضان محمد بطيخ:** الوسيط في القانون الإداري، دار النهضة العربية، القاهرة، ١٩٩٧م.
- **د. سعاد الشرقاوى:** القانون الإدارى، القاهرة، دار النهضة العربية، ١٩٨٣.
- **د. سليمان محمد الطماوى:** الوجيز فى القانون الإدارى «دراسة مقارنة»، القاهرة، دار الفكر العربى، ١٩٧٩.
- **د. طعيمة الجرف:** القانون الإدارى والمبادئ العامة فى تنظيم ونشاط السلطات الإدارية، القاهرة، دار النهضة العربية، ١٩٧٨.

- **د. عبد الفتاح بيومي حجازي:** الحكومة الإلكترونية ونظامها القانوني، الكتاب الأول، النظام القانوني للحكومة الإلكترونية، دار الفكر الجامعي، الإسكندرية، ٢٠٠٦م
  - قاموس لسان العرب، الجزء التاسع، القاهرة، الدار المصرية للتأليف والترجمة.
  - قاموس مختار الصحاح، الطبعة الثالثة.
- **د. محمد أنس قاسم جعفر:** الوسيط فى القانون العام «أسس وأصول القانون الإدارى»، بدون سنة نشر.
- **د. محمد عبد الحميد أبوزيد،** الطابع القضائي للقانون الإداري – دراسة مقارنة، «د.ط»، دار الثقافة العربية، القاهرة، ١٩٨٤م.
- **د. محمد عبدالله الحراري،** أصول القانون الإداري الليبي، الجزء الأول، تنظيم الإدارة الشعبية ووظائفها، الطبعة الثالثة، ١٩٩٨.
- **د. محمد محمود المكاوي،** الإدارة الإلكترونية، دون طبعة، دار الفكر والقانون، الإسكندرية، ٢٠١١.
- **د. محمود سعد الدين الشريف:** النظرية العامة للضبط الإدارى، مقالة منشورة بمجلة مجلس الدولة، السنة الحادية عشرة، ١٩٦٢.
- **د. محمود عاطف البنا:** الوسيط فى القانون الإدارى، القاهرة، دار الفكر العربى، ١٩٨٤.
- **د. ناجح أحمد عبد الوهاب:** التطور الحديث للقانون الإداري في ظل نظام الحكومة الإلكترونية، «دون طبعة»، دار النهضة العربية- القاهرة، ٢٠١٢.
- **د. هدى قشقوش:** جرائم الحاسب الآلى فى التشريع المقارن – دار النهضة العربية – القاهرة – ١٩٩٢.

رسائل وأبحاث:

- **أعـاد علـى الحمـود القيسي،** النمـوذج الإلكـتروني الموحد للقـرارات الإدارية، بحث مقـدم للمؤتمر العلمي السنوي (١٧) بعنـوان المعاملات الإلكترونية، كلية القانـون- جامعة الإمارات ومركز الإمارات للدراسـات والبحوث الاستراتيجية، أبو ظبي، ١٩-٢٠/٥/٢٠٠٩م.
- **حمـدي سليمان القبيلات،** التوقيع كشكليـة في القرار الإداري الإلكتروني، بحث منشـور بمجلة دراسات علوم الشريعـة والقانون، صادرة عن عمـادة الدراسات العليا بالجامعة الأردنية بعمان، المجلد رقم ٣٤، (ملحق) ٢٠٠٧م.
- **طارق محمد عبد القادر عبد الله،** القيود التي ترد على حرية القاضي في التعبير وإبـداء الرأي المخالف – دراسـة تطبيقية في القضاء الدستوري، رسالة مقدمة للحصـول على درجة الدكتوراه في القانون بكليـة الحقوق، من جامعة القاهرة، ١٤٣٣هـ - ٢٠١٢م.
- **عبـد الله بـن سعيد آل دحـوان،** دور إدارة التطويـر الإداري فـي تطبيق الإدارة الإلكترونية- رسالة ماجستير، جامعة الملك سعود، بالرياض، ١٤٢٩هـ/-٢٠٠٨م.
- **عثمـان زعل فارس المعايطـة،** الحكومة الإلكترونية وأثرهـا على المرافق العامة- دراسـة مقدمة لنيل درجة الماجستير في القانون العام من كلية الحقوق، بجامعة القاهرة، ٢٠٠٩م-٢٠١٠م.
- **علاء محيي الدين مصطفى أبو أحمد،** القرار الإداري الإلكتروني كأحد تطبيقات الحكومـة الإلكترونية، بحث مقدم للمؤتمـر العلمي السنوي ١٧ بعنوان المعاملات الإلكترونيـة، كلية القانون بجامعة الإمارات ومركز الإمارات للدراسات والبحوث الاستراتيجية بأبو ظبي، ١٩-٢٠/٥/٢٠٠٩م.
- **محمـد سليمان نايـف شبير،** أثر التطـور الإلكتروني على التصرفـات القانونية لـلإدارة فـي دولة فلسطين- بحث منشـور- مجلة جامعـة الأزهر-غزة، سلسلة العلوم الإنسانية- ٢٠١٥م، المجلد رقم (١٧)، العدد رقم (٢ / ب).
- **محمد سليمان نايف شبير،** النفاذ الإلكتروني للقرار الإداري- رسالة دكتوراه في القانون العام، كلية الحقوق-جامعة عين شمس، القاهرة ٢٠١٥.

- **د. عبـادة أحمد عبادة:** التدمير المتعمد لأنظمـة المعلومات الإليكترونية – بحث منشـور لدى مركـز البحوث والدراسـات، الإدارة العامة لشرطـة دبى – مارس ١٩٩٩.
- **د. محمـد الأمين البشرى:** «التحقيق فى جرائـم الحاسب الآلي» بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، مقدم إلى كلية الشريعة والقانون – جامعة الإمارات العربية المتحدة – الفترة من ١-٣ مايو ٢٠٠٠م.

مراجع أخرى:

- **حسين بن محمد الحسن،** الإدارة الإلكترونية بين النظرية والتطبيق، ورقة مقدمة إلى المؤتمـر الـدولي للتنمية الإداريـة (نحو أداء متميز فـي القطاع الحكومي)، (الرياض)- ١٦/١٣ ذو القعدة ١٤٣٠هـ الموافق ١-٤ نوفمبر- ٢٠٠٩م.
- **يوسـف شباط،** موعد الطعن في دعوى الإلغـاء ودوره في توطيد سيادة القانون، بحث منشور، مجلـة جامعة دمشق للعلوم الاقتصاديـة والقانونية، المجلد الأول، العدد الأول، ١٩٩٩.
- حكـم المحكمـة الإداريـة العليا فـى القضية ١٥١٧ لسنـة ٢ق، والصـادر بجلسة ١٣/٤/١٩٥٧، منشـور بمجموعـة المبـادئ التـى قررتها المحكمـة الإدارية العليا للسنة الثانية تحت رقم ٩٣.

ثانياً- باللغة الإنجليزية والفرنسية:

- Berr – Gabal, le controle de l›administration par la commission national de l'informatique et des libertes, R.D.P. 1980.
- BLAEVOET (C.): Des recours juridictionnels contre les mesures de police, Th, Paris, 1908, pp. 1415-.
- Dogin, Henry S., Computer crime: Criminal justice resource manual Washington. D.C.U.S. Government printing office, 1996.
- KLEIN (C.): «La police du domaine public», Paris, L.G.D.J., 3e ed, 1966.
- PAPANICOLAIDIS (D.) : Introduction générale à la théorie de la police administrative, Th, Paris, 1958, L.G.D.J., ed. 1960.