سلطات مأموري الضبط القضائي في جرائم الانترنت والهاتف

د. نديم محمد حسن الترزي
أستاذ القانون الجنائي المساعد بأكاديمية الشرطة
عنوان المراسلة: altarziyemen@yahoo.com

ملخص البحث:

أصبحت دراسة موضوع اختصاصات مأمور الضبط القضائي في جرائم الانترنت والهاتف من الدراسات الهامة، نتيجة قلة إلمام مأموري الضبط القضائي بالجرائم المتعلقة بهذه الوسائل، ولما لهذه الوسائل من تأثير خطير على الأمن القومي للدول، وكذلك على الجوانب الاقتصادية للشركات والأشخاص، ومساسها أيضاً بحرمة الحياة الخاصة.

وقد أظهرت هذه الدراسة أيضاً وجود مشكلة أخرى تتمثل في افتقار التشريعات الجنائية اليمنية إلى النصوص القانونية التي تعالج مثل هذه المسائل.

لذا فإن هذه الدراسة هدفت إلى توضيح اختصاصات مأموري الضبط القضائي حيال هذه الجرائم، وفهم النصوص القانونية التي تحكم هذه المسائل، والقصور فيها، والتوصيات المقترحة لمعالجة هذا القصور.

Authorities of Judicial Arrest Officers in the Cybercrimes and Mobile Crimes

Abstract:

The topic of the of judicial arrest officers in cybercrimes and mobile crimes has increasingly become very important to many researchers and respective authorities due to the lack of knowledge and awareness of judicial arrest officers about the crimes relating to these tools and due to its dangerous impact on the national security of the state and on the economic aspects of the companies and business individuals and their privacy.

This study also showed another problem which is that the Yemeni criminal legislations lack to the legal provisions that address such types of crimes.

This study aimed to explore the competence of the judicial arrest officers in such types of crimes and investigate the legal provisions in force that regulate these issues and any deficiency and the proposed recommendations that help to address such deficiencies or shortcoming in dealing with any cybercrime.

مقدمة:

توسع مفهوم تكنولوجيا المعلومات، فلم يعد قاصراً على الحاسوب الآلي، بل أصبح يشمل جميع الوسائل الإلكترونية، وشبكات الاتصال، وقد كان لهذا التوسع في مجال تكنولوجيا المعلومات تأثير كبير في توسع الجرائم الإلكترونية، وخاصة الجرائم التي ترتكب بواسطة شبكة الإنترنت، والتي أصبحت ذات تأثير خطير على الأمن القومي للدول، وكذلك على الجوانب الاقتصادية للشركات والأشخاص، وتمس أيضاً حرمة الحياة الخاصة، نظراً لوجود الثغرات الفنية فيها.

وكذلك الحال في جرائم الهاتف فقد أصبحت أداة سهلة في ارتكاب بعض الجرائم لما تتميز به من تقنية سهلة التناول.

ولا شك أن التطور المستمر في تكنولوجيا المعلومات جعل مهمة رجال العدالة – ومنهم مأموري الضبط القضائي – في اكتشاف الجرائم الإلكترونية أصعب من ذي قبل، إذ لا يكفي أن يكون مأمور الضبط القضائي ملماً بالجوانب القانونية فحسب، بل يجب أن تكون لديه الخبرة اللازمة للتعامل مع مثل هذه الجرائم.

ومما يزيد الأمر تعقيداً عدم مسايرة التشريعات الجنائية للتطور المتسارع في تكنولوجيا المعلومات، وما صاحب ذلك من تزايد في ارتكاب العديد من الجرائم بأساليب تقنية عالية يصعب اكتشافها.

وبما أن القانون الجنائي – ومنه قانون الإجراءات الجزائية – يكاد يفتقر إلى نصوص قانونية تساير التطور المتسارع في تكنولوجيا المعلومات، وما أدت إليه من ارتكاب جرائم غير تقليدية بدقة تقنية عالية، فإنه لابد من البحث في قانون الإجراءات الجزائية عن نصوص قانونية – وإن كانت تتسم بالعمومية والتقليدية – تعالج مثل هذه الجرائم، حتى يتم تعديل القانون وإدخال نصوص تعالج مثل هذه القضايا.

أولاً: مشكلة الدراسة

تُعد الجرائم الإلكترونية – ومنها جرائم الإنترنت والهاتف – جرائم حديثة ومعقدة، لاسيما بالنظر إلى اسلوب ارتكابها أو وسائل كشفها، لذلك فإن خبرات معظم مأموري الضبط القضائي لا تزال قاصرة عن مسايرة التقدم التكنولوجي في مجال مكافحة الجريمة الإلكترونية، وهي في غالبيتها جرائم عابرة للحدود (Transnational).

وهذه الفجوة بين مستوى تطور الجريمة الالكترونية والمستوى المتدني في خبرات مأموري الضبط القضائي تمثل المشكلة الأولى.

كما تُظهر الجرائم الإلكترونية مشكلة أخرى تتمثل في عدم وجود نصوص قانونية في القانون الجنائي اليمني – ومنه قانون الإجراءات الجزائية – تنظم هذا النوع من الجرائم بشكل مباشر، وإنما مجرد نصوص عامة.

ثانياً: أهمية الدراسة

تكتسب هذه الدراسة أهميتها من كون الجريمة الالكترونية تُلحق الضرر بالكثير من الناس الذين يتعاملون بشبكات الإنترنت والهاتف، ويتعرضون للكثير من الجرائم من قبل أشخاص لهم قدرة عالية في مجال التقنية.

كما تبرز أهميتها أيضاً في إلقاء الضوء على النصوص التشريعية في قانون الإجراءات الجزائية من حيث مدى ملاءمتها لهذه الجرائم المستحدثة، وكذا مدى كفايتها.

فضلاً عن محاولة تسليط الضوء على الدور الذي يجب أن يقوم به مأموري الضبط القضائي لمواجهة مثل هذه الجرائم.

ثالثاً: أهداف الدراسة

تهدف هذه الدراسة إلى تحقيق ما يلي:

1 - الكشف عن مدى كفاية نصوص قانون الإجراءات الجزائية لمواجهة الجرائم الالكترونية، وبيان القصور فيها، ووضع التوصيات المناسبة لذلك.
2 - توضيح دور مأموري الضبط القضائي في مواجهة جرائم الإنترنت والهاتف.
3 - وضع التصورات المناسبة للمواجهة القانونية لجرائم الإنترنت والهاتف.

رابعاً: تساؤلات الدراسة

تجيب هذه الدراسة على التساؤلات الآتية:

1 - ما مدى ملاءمة نصوص قانون الإجراءات الجزائية لمواجهة جرائم الإنترنت والهاتف؟ وما مدى كفايتها؟

2 - ما هو دور مأموري الضبط القضائي في مواجهة جرائم الإنترنت والهاتف؟

3 - ما هو الجزاء المترتب على مخالفة مأموري الضبط القضائي لواجباتهم؟

خامساً: منهجية الدراسة

نظراً لأهمية هذه الدراسة كونها تبحث في موضوع الجرائم الالكترونية المرتكبة بواسطة شبكات الإنترنت والهاتف، وما تتطلبه هذه الجرائم من خبرة فنية دقيقة لدى رجال العدالة – ومنهم مأموري الضبط القضائي – وكذا مواكبة التشريعات لهذا النوع من الجرائم، فإنني سأتناول هذه الدراسة باستخدام المنهج الوصفي والتحليلي.

سادساً: خطة الدراسة

إن دراسة مسئولية مأموري الضبط القضائي في جرائم الانترنت والهاتف تستدعي تقسيمها إلى ثلاثة مباحث نتناول الإطار التشريعي لجرائم الإنترنت والهاتف والتحديات الفنية والإجرائية في المبحث الأول، نخصص المطلب الأول منه للحديث عن مدى ملاءمة وكفاية نصوص قانون الإجراءات الجزائية لمواجهة جرائم الإنترنت والهاتف، وفي المطلب الثاني نتناول التحديات الفنية والإجرائية في جرائم الانترنت والهاتف.

وفي المبحث الثاني نتناول اختصاصات مأموري الضبط القضائي في جرائم الإنترنت والهاتف والشروط والقواعد الواجب مراعاتها، ونخصص المطلب الأول منه لتناول اختصاصات مأموري الضبط القضائي في مواجهة جرائم الإنترنت والهاتف، أما المطلب الثاني فنخصصه للحديث عن الشروط والقواعد الواجب مراعاتها أثناء مباشرة إجراءات الاستدلال في جرائم الإنترنت الهاتف.

أما في المبحث الثالث فسنتناول الجزاء المترتب على مخالفة مأموري الضبط القضائي للقواعد الاجرائية، على أن يكون المطلب الأول لدراسة الجزاء الاجرائي المترتب على مخالفة مأموري الضبط القضائي للقواعد الإجرائية (بطلان الدليل)،

ويخصص المطلب الثاني لدراسة الجزاء الجنائي والمدني المترتب على مخالفة مأموري الضبط القضائي للقواعد الاجرائية.

وفي الأخير نتناول خاتمة هذه الدراسة والتي تتضمن مجموعة من النتائج والتوصيات.

المبحث الأول

الإطار التشريعي لجرائم الإنترنت والهاتف والتحديات الفنية والإجرائية

تمهيد وتقسيم:

بات من الواضح في الآونة الأخيرة تزايد الجرائم الإلكترونية (Cybercrime)، خاصة تلك التي تقع بواسطة الإنترنت والهاتف، مما أدى إلى تعاظم دور الدليل الرقمي في كشف الجرائم الواقعة بواسطة هذه الوسائل.

وبما أن هذه الجرائم تُعد من الجرائم الحديثة، فإن الوسائل والأساليب المستخدمة في ارتكاب هذه الجرائم لم تكن معروفة لدى المشرع وقت وضع التشريع.

والسؤال الذي يجب طرحه في مثل هذه الحالة هو: ما مدى ملاءمة وكفاية النصوص الحالية في قانون الإجراءات الجزائية لمواجهة هذه الجرائم؟ وما هي التحديات الفنية والإجرائية التي تظهر أثناء التعامل مع الجرائم؟

هذا ما سنبينه في هذا المبحث، من خلال تقسيمه إلى مطلبين على النحو الآتي:

المطلب الأول: مدى ملاءمة وكفاية نصوص قانون الإجراءات الجزائية لمواجهة جرائم الإنترنت والهاتف.

المطلب الثاني: التحديات الفنية والإجرائية في جرائم الانترنت والهاتف.

المطلب الأول
مدى ملاءمة وكفاية نصوص قانون الإجراءات الجزائية لمواجهة جرائم الإنترنت والهاتف

تُعد الجمهورية اليمنية من الدول التي لم تخصص قانوناً لمواجهة الجرائم الإلكترونية – ومن بينها جرائم الإنترنت والهاتف – كما لم تسن نصوصاً خاصة بهذه الجرائم ضمن نصوص قانون الإجراءات الجزائية، وما ورد في هذا القانون عبارة عن نصوص عامة تضع قواعداً عامة للتعامل مع وسائل الاتصال، مع إيراد بعض القواعد الإجرائية التي تُعنى بالتعامل مع جرائم الهاتف ونوضح كل ذلك فيما يلي:

أولاً: النصوص الإجرائية التي حددت الجرائم الواقعة بواسطة وسائل الاتصال:

أورد قانون الإجراءات الجزائية نصوصاً عدة تكفل المحافظة على حرمة الحياة الخاصة، فقد نصت المادة (2/12) منه، على أن: "حرية وسرية المراسلات البريدية والسلكية واللاسلكية وكافة وسائل الاتصال مكفولة وفقاً للدستور، ولا يجوز مراقبتها أو تفتيشها أو إفشاء سريتها أو تأخيرها أو مصادرتها إلا في الحالات التي بينها القانون، وبأمر من النيابة العامة أو المحكمة المختصة" ([1]).

كما نصت المادة (14) منه أيضاً على أنه: "لا يجوز المساس بحرمة الحياة الخاصة للمواطن في غير الأحوال المصرح بها في هذا القانون، ويعتبر مساساً بها ارتكاب أحد الأفعال الآتية:

1 - استراق السمع أو تسجيل أو نقل المحادثات التي تجري في مكان خاص أو عن طريق الهاتف أو عن طريق جهاز من الأجهزة أياً كان نوعه.
2 - التقاط أو نقل صورة شخص في مكان خاص بجهاز من الأجهزة أياً كان نوعه.
3 - الإطلاع على الخطابات أو الرسائل أو البرقيات أو مصادرتها.

---

[1] القرار الجمهوري رقم (13) لسنة 1994م بشأن الاجراءات الجزائية.

ونصت المادة (131) منه على أن: "للأشخاص والمساكن والمراسلات البريدية والمحادثات السلكية واللاسلكية والمحادثات الشخصية حرمة.. وحرمة المراسلات تمنع من الإطلاع عليها أثناء نقلها أو انتقالها من شخص إلى آخر بريدية كانت أو هاتفية".

ويتبين من هذه النصوص أن قانون الإجراءات الجزائية لم ينص بشكل صريح على الجرائم الالكترونية، وإنما أشارت إلى بعض الجرائم؛ كالتقاط الصور أو نقلها، وكذا الإطلاع على الخطابات أو الرسائل أو البرقيات أو مصادرتها، وهذه الجرائم قد ترتكب بواسطة الإنترنت، وقد ترتكب أيضاً بالوسائل التقليدية.

أما الجرائم التي ترتكب بواسطة الهاتف فقد بينتها هذه النصوص في تسجيل أو نقل المحادثات أو الاطلاع على الرسائل، ولكن لم تشر هذه النصوص إلى بقية الجرائم التي ترتكب بواسطة الهاتف.

ثانياً: النصوص الإجرائية التي حددت اختصاص مأموري الضبط القضائي:

نظراً لحداثة جرائم الإنترنت والهاتف فلم يكن المشرع لنصوص قانون الإجراءات الجزائية على علم بها عند سن هذا التشريع، لذلك جاءت هذه النصوص قاصرة عن مواجهة الجرائم المرتكبة بواسطة هذه الوسائل، كما أنها لم تحدد اختصاصات مأموري الضبط القضائي في مواجهة هذه الجرائم بشكل مباشر، وإنما حددت اختصاصات عامة لمأموري الضبط القضائي في جميع الجرائم، إذ نصت المادة (91 أ.ج) على أن: "مأمورو الضبط القضائي مكلفون باستقصاء الجرائم وتعقب مرتكبيها وفحص البلاغات والشكاوى وجمع الاستدلالات والمعلومات المتعلقة بها وإثباتها في محاضرهم وإرسالها إلى النيابة العامة".

كما أن قانون الإجراءات الجزائية جعل مباشرة إجراءات الاطلاع على المراسلات البريدية أو تسجيل المحادثات السلكية أو اللاسلكية من قبل النيابة العامة أثناء التحقيق أو من القاضي أثناء المحاكمة، وهذا ما أكدته المادة (132 أ.ج)، إذ نصت على أنه: "لا يجوز تفتيش الأشخاص أو دخول المساكن أو الاطلاع على المراسلات البريدية، أو تسجيل المحادثات السلكية أو اللاسلكية.. إلا بأمر

من النيابة العامة أثناء التحقيق ومن القاضي أثناء المحاكمة".

ونصت المادة (146 أ.ج) على أن: "لعضو النيابة العامة المختص وحده الاطلاع على الخطابات والرسائل والبرقيات.. ويجوز بأمر من رئيس النيابة تكليف أحد رجال إدارة الهاتف بعد تحليفه اليمين القانونية بالاستماع إلى المحادثات الهاتفية وتسجيلها لنقل مضمونها إليه..".

كما نصت المادة (148 أ.ج) على أن: "للنيابة العامة أن تأمر بضبط جميع الخطابات والرسائل والصحف والمطبوعات لدى مكاتب البرق، وأن تأمر بمراقبة المحادثات السلكية واللاسلكية...".

ويتضح من خلال هذه النصوص أن قانون الإجراءات الجزائية لم يُشر إلى اختصاصات مأموري الضبط القضائي في مواجهة جرائم الإنترنت والهاتف، وإنما وردت نصوص عامة تحدد اختصاصات مأموري الضبط القضائي في أعمال الاستدلالات في جميع الجرائم، ولكنها لا تكفي لمواجهة الجرائم الإلكترونية، نظراً لما يصاحب هذه الجرائم من أساليب تقنية تحتاج إلى دقة في صياغة النصوص. كما أن مشروع تعديل قانون الجرائم والعقوبات اليمني المرفوع من وزير العدل إلى مجلس النواب بتاريخ 2010/4/7م لم يتضمن أي تعديلات أو نصوصاً إضافية لمواجهة هذا النوع من الجرائم.

المطلب الثاني
التحديات الفنية والإجرائية في جرائم الانترنت والهاتف

تكشف الجرائم الالكترونية – ومنها جرائم الإنترنت والهاتف – الكثير من التحديات التي تتعلق بطبيعتها التقنية الدقيقة أو بإجراءات اكتشافها وجمع الأدلة فيها، وترجع هذه التحديات إلى حداثة هذا النوع من الجرائم نسبياً، وكذا القصور في إجراءات مأموري الضبط القضائي وقدراتهم في مواجهة هذه الجرائم، لذلك سنتناول التحديات الفنية المرتبطة بجرائم الإنترنت والهاتف، ومن ثم التحديات الاجرائية المرتبطة بإجراءات مأموري الضبط القضائي في مواجهة جرائم الانترنت والهاتف، وذلك على النحو الآتي:

أولاً: التحديات الفنية المرتبطة بجرائم الإنترنت والهاتف

جرائم الإنترنت والهاتف – كغيرها من الجرائم الالكترونية – ذات طبيعة خاصة، لأنها تتم في العالم الافتراضي أو الفضاء السيبراني (Cyber space)، وهو ما يجعلها أكثر تعقيداً من الجرائم التقليدية، من حيث اكتشافها والاجراءات المتعلقة بضبطها، لذلك فإن أهم هذه التحديات تظهر فيما يلي:

1 - **قابلية جرائم الإنترنت والهاتف للمعالجة الإلكترونية للبيانات**:

جرائم الإنترنت والهاتف كغيرها من الجرائم المعلوماتية تتم بالمعالجة الإلكترونية للبيانات وإخراجها بالكيفية التي يرغب بها مستخدمها، فالمجرم المعلوماتي في جرائم الانترنت يتدخل في مجال المعالجة الإلكترونية للنصوص والكلمات والأرقام بفضل الخصائص المتوفرة في النظام الآلي، من إمكانية التصحيح والتعديل والمحو والتخزين والاسترجاع والطباعة ليخرجها في النهاية بالصورة التي يريدها[1]، كذلك الحال في جرائم الهاتف يستطيع المجرم المعلوماتي التلاعب في ارسال الرسائل النصية من خلال عدة وسائل، كالإنترنت أو عن طريق مزود الخدمة (Service Provider) في شركات الهاتف المحمول.

---

(1) للمزيد أنظر: محمد علي العريان، الجرائم الإلكترونية، دار الجامعة الجديدة للنشر، الإسكندرية، طبعة 2004م، ص47.

2 - **صعوبة اكتشاف جرائم الإنترنت والهاتف:**

الجرائم المعلوماتية بشكل عام من الجرائم التي يصعب اكتشافها، ذلك أن الجاني في الجرائم المعلوماتية يتسم بالمكر والدهاء والاحتيال باستخدام تقنيات معلوماتية عالية الكفاءة، إلى جانب ذلك فإنها تمتاز بالسرعة الفائقة التي تمكنه من ارتكاب جريمته[1]، كما تمتاز أيضاً بأن آثارها تظهر عادةً بعد حين، ولا نلاحظ الجريمة ذاتها، فنحن نعرف بحدوث جريمة الكترونية من خلال ما يترتب عليها من آثار، وليس وقت حدوثها، كما هو الحال في نقل الأموال.

وكذا يستطيع مرتكب هذه الجرائم تشفير هذه البيانات في جرائم الإنترنت، مما يؤدي إلى وجود مصاعب حقيقية بشأن إقامة الدليل على ارتكاب هذه الجرائم والأشخاص المشتركين في ارتكابها[2].

3 - **جرائم عابرة الحدود:**

غالبية الجرائم المعلوماتية – ومنها جرائم الإنترنت والهاتف – تعتبر جرائم عابرة الحدود، إذ قد ترتكب من قبل أشخاص من خارج الحدود، أو أنها تمر عبر شبكات وأنظمة معلومات خارج الحدود، وأن مرتكبها شخص داخل حدود الدولة ذاتها[3]. وبمعنى آخر يكون الفعل الإجرائي في هذا النوع من الجرائم باستخدام وحدات طرفية أو اتصال هاتفي، يمكن للجاني من خلالها إعطاء تعليمات عبر الوسائل الإلكترونية تمكنه من اختراق شبكات المعلومات في أي مكان في العالم، والنتيجة هي صعوبة الوصول إليه أو صعوبة التحقق من الدليل[4].

---

(1) د. سعيد عبداللطيف حسن, إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت, دار النهضة العربية, القاهرة, الطبعة الأولى, عام 1999م, ص95.

(2) د. حسين بن سعيد الغافري, السياسة الجنائية في مواجهة جرائم الإنترنت, دار النهضة العربية, القاهرة, طبعة 2009م, ص561.

(3) عبدالله عبدالكريم عبدالله, جرائم المعلوماتية والإنترنت, منشورات الحلبي الحقوقية, بيروت, لبنان, الطبعة الأولى, 2007م, ص48.

(4) للمزيد أنظر: د. سعيد عبداللطيف حسن, مرجع سابق, ص96.

4 - **صعوبة الاثبات**:

إن صعوبة الاثبات تمثل تحدياً جدياً في محاربة الجريمة المعلوماتية؛ ليس بسبب تدني القدرات الفنية لمأموري الضبط القضائي فحسب، وإنما أيضاً بسبب سهولة محو الدليل أو اتلافه في زمن قصير جداً، لذلك يحتاج الاثبات في الجريمة المعلوماتية إلى قدرات فنية عالية المستوى؛ تساوي أو تفوق قدرات الفاعل في الجريمة المعلوماتية.

5 - **طبيعة مسرح الجريمة**:

الجرائم المعلوماتية – ومنها جرائم الانترنت والهاتف – تتم في الفضاء السيبراني (Cyber space) أو العالم الافتراضي (Vertual World)، وهذا يعني أن الفاعل قد يرتكب الجريمة عن بعد في بلد تبعد آلاف الكيلومترات عن مكان وجوده، دون الحاجة إلى الانتقال إلى مسرح الجريمة، كما أن الجريمة المعلوماتية ناعمة (soft) لا يوجد بها استخدام للعنف، وبالتالي ينعدم الدليل المادي المألوف في الجريمة التقليدية، ومن هنا تظهر صعوبة التعامل مع مسرح الجريمة المعلوماتية.

ثانياً: التحديات الإجرائية المرتبطة بإجراءات مأموري الضبط القضائي:

لاشك أن جرائم الإنترنت والهاتف – كغيرها من الجرائم المعلوماتية – هي جرائم حديثة بالنسبة لمأموري الضبط القضائي، **لاسيما** في كيفية استخلاص الدليل في هذه الجرائم، لذلك فإن التحديات المرتبطة بإجراءات مأموري الضبط القضائي تظهر فيما يلي:

1 - **نقص الخبرة لدى مأموري الضبط القضائي في مواجهة جرائم الإنترنت والهاتف**:

جرائم الإنترنت والهاتف – كما سبق – ذات طبيعة خاصة، نظراً للتقنية العالية المستخدمة في ارتكابها، وهذا يتطلب وجود أشخاص لديهم مهارات وبرامج تخصصية دقيقة لاكتشافها وضبطها[1].

---

(1) حول هذا الموضوع أنظر: د.عبدالفتاح بيومي حجازي, مبادئ الإجراءات الجنائية في جرائم الكمبيوتر, دار الكتب القانونية, مصر, طبعة 2007م, ص55.

إلا أن معظم مأموري الضبط القضائي في الجمهورية اليمنية يعانون من نقص الخبرة فيما يتعلق بهذا النوع من الجرائم، وكيفية اكتشافها والتعامل معها، نظراً لأن الجرائم المعلوماتية حديثة النشأة، كما أن الجرائم المعلوماتية – ومنها جرائم الإنترنت والهاتف – تتقدم بسرعة هائلة توازي سرعة تقدم تقنية المعلومات ذاتها[1]، لذلك من الضروري تدريب وتأهيل مأموري الضبط القضائي على الأساليب الفنية المستخدمة في ارتكاب هذه الجرائم وطرق الكشف عنها وكيفية التحفظ عليها[2].

2- **القصور التشريعي في مواجهة جرائم الإنترنت والهاتف:**

من التحديات التي تواجه مأموري الضبط القضائي في الجرائم المعلوماتية في بلادنا – ومنها جرائم الإنترنت والهاتف – عدم وجود نصوص قانونية تواجه بشكل مباشر هذا النوع من الجرائم، نظراً لحداثة هذا الموضوع نسبياً، لذلك أصبحت النصوص القانونية الجنائية – ومنها نصوص قانون الإجراءات الجزائية اليمني – عاجزة وغير قادرة على الإحاطة بكافة جوانب هذه الجرائم، وهذا ما يتطلب وجود تشريعات تكفل تجريم هذه الجرائم وتحدد كيفية الحصول على دليل ارتكابها[3].

3- **تنوع واختلاف النظم القانونية الإجرائية:**

يظهر في مجال مواجهة الجرائم المعلوماتية تحدي آخر يتمثل في تنوع واختلاف النظم القانونية الإجرائية التي تواجه هذا النوع من الجرائم، إذا أن بعض الدول تعتبر بعض الإجراءات التي تنفذ لاكتشاف الجرائم المعلوماتية –

---

(1) د.عبدالفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، لم يحدد الناشر ومكان النشر، 2009م، ص81.

(2) د. سعيد عبداللطيف حسن، مرجع سابق، ص129.

(3) للمزيد أنظر: د. هدى حامد قشقوش، جرائم الحاسب الإلكتروني، دار النهضة العربية، القاهرة، طبعة 1992م، ص16. محمد علي العريان، مرجع سابق،ص25.

ومنها جرائم الإنترنت والهاتف – من إجراءات الاستدلال، بينما في دول أخرى قد تكون هذه الإجراءات من إجراءات التحقيق[1].

وبمطالعة قانون الإجراءات الجزائية اليمني نجد أنه حدد بأن إجراءات التحري والمعاينة من إجراءات الاستدلال حسب ما نصت عليه المادة (92) منه، لكن المعاينة والتحري في مجال الجرائم المعلوماتية تتطلب التفتيش في الأجهزة المستخدمة في ارتكاب الجرائم، وهذا ينقلنا إلى إجراءات التحقيق التي تختص بها النيابة العامة، وهذا يُعد من العوائق أو التحديات التي تواجه مأموري الضبط القضائي.

(1) د. حسين بن سعيد الغافري، مرجع سابق، ص692.

المبحث الثاني
اختصاصات مأموري الضبط القضائي في جرائم الإنترنت والهاتف والشروط والقواعد الواجب مراعاتها

تمهيد وتقسيم:

أضفى القانون في المادة (84.أ،ج) صفة الضبطية القضائية على مأموري الضبط القضائي لمباشرة إجراءات الضبطية القضائية في مواجهة مرتكبي الجرائم بمختلف أنواعها، وهذا ما أوضحته المادة (91. أ،ج) والتي نصت على أن: "مأمورو الضبط القضائي مكلفون باستقصاء الجرائم وتعقب مرتكبيها وفحص البلاغات والشكاوى وجمع الاستدلالات والمعلومات المتعلقة بها وإثباتها في محاضرهم وإرسالها إلى النيابة العامة".

ولاشك أن جرائم الإنترنت والهاتف من الجرائم المستحدثة التي تزيد من الأعباء الملقاة على عاتق مأموري الضبط القضائي، نظراً لعدم وجود نصوص صريحة تحدد مسئولية مأموري الضبط القضائي في مواجهة هذه الجرائم، وللطبيعة الخاصة التي تتميز بها هذه الجرائم، والأساليب الحديثة والمتطورة التي ترتكب بواسطتها، التي جعلت مهمة مأموري الضبط القضائي صعبة في مواجهة هذه الجرائم.

وللمزيد من البيان حول مسئولية مأموري الضبط القضائي في مواجهة الجرائم، فإنني سأتناول هذا المبحث في مطلبين على النحو الآتي:

المطلب الأول: اختصاصات مأموري الضبط القضائي في مواجهة جرائم الإنترنت والهاتف.

المطلب الثاني: الشروط والقواعد الواجب مراعاتها أثناء مباشرة إجراءات الاستدلال في جرائم الإنترنت والهاتف.

المطلب الأول

اختصاصات مأموري الضبط القضائي في مواجهة جرائم الإنترنت والهاتف

مأمورو الضبط القضائي هم من أوكل إليهم القانون التحري عن الجرائم وتعقب مرتكبيها وفحص البلاغات والشكاوي وجمع الاستدلالات والمعلومات المتعلقة بها، وإثباتها في محاضرهم، وإضافة إلى ذلك منحهم القانون اختصاصات استثنائية في حالة الجريمة المشهودة، وفي حالة الندب للتحقيق، وهذا ما أشارت إليه المواد (99، 108، 117. أ.ج)، لذلك فإننا في هذا المطلب سنتناول الاختصاصات الأصلية والاستثنائية لمأموري الضبط القضائي في مواجهة جرائم الإنترنت والهاتف، وذلك على النحو الآتي:

أولاً: الاختصاصات الأصلية لمأموري الضبط القضائي في مواجهة جرائم الإنترنت والهاتف:

لم يحدد القانون اليمني صراحة الدور المناط بمأموري الضبط القضائي في مواجهة جرائم الإنترنت والهاتف، وإنما نص على اختصاص مأموري الضبط القضائي بمباشرة إجراءات الاستدلال في المادة (91.أ.ج)، إذ نصت على أن: "مأمورو الضبط القضائي مكلفون باستقصاء الجرائم وتعقب مرتكبيها وفحص البلاغات والشكاوى وجمع الاستدلالات والمعلومات المتعلقة بها وإثباتها في محاضرهم وإرسالها إلى النيابة العامة".

وتأسيسياً على ذلك، فإن دور مأموري الضبط القضائي هو جمع المعلومات عن الجريمة وتعقب مرتكبيها – بالإضافة إلى الإجراءات الأخرى التي حددتها المادة السالفة الذكر عن طريق الأساليب القانونية[1].

ومن المعروف أن المعاينة من أهم إجراءات الاستدلال لجمع المعلومات عن الجريمة من مسرح الجريمة، ولكن معاينة مسرح الجريمة في جرائم الإنترنت تختلف عن المعاينة في مسرح الجريمة التقليدية، إذ تتميز جرائم الإنترنت والهاتف– كغيرها من الجرائم المعلوماتية – بطبيعتها الخاصة وأسلوبها المتطور، وترتكب

(1) د. حسين بن سعيد الغافري، مرجع سابق، ص444.

بأدوات خاصة يملكها الشخص؛ كالكمبيوتر والهاتف الشخصي المحمول الذي يملكه مرتكب الجريمة. وقد نظم القانون الحماية التشريعية لوسائل الاتصالات التي تحد من صلاحيات مأموري الضبط القضائي في هذا الصدد، إذ أن المعاينة في جرائم الإنترنت والهاتف تعني البحث والتفتيش في أجهزة الكمبيوتر والهاتف التي تستخدم في ارتكاب الجرائم، وهذه الإجراءات من اختصاص سلطة التحقيق، وهذا ما أشارت إليه المادة (2/12 أ.ج) والتي نصت على أن: "حرية وسرية المراسلات البريدية واللاسلكية وكافة وسائل الاتصال مكفولة وفقاً للدستور، ولا يجوز مراقبتها أو تفتيشها أو إفشاء سريتها أو تأخيرها أو مصادرتها إلا في الحالات التي يبينها القانون وبأمر من النيابة العامة أو من المحكمة المختصة".

وبناءً على ما سبق، فإن اختصاص مأمور الضبط القضائي في جرائم الإنترنت والهاتف يتمثل في إجراءات الاستدلال التي حددها قانون الإجراءات الجزائية، إلا أن المعاينة – مع أنها من إجراءات الاستدلال – تتطلب التفتيش في أجهزة الكمبيوتر والهاتف كونها أدوات الجريمة، والتفتيش يُعد من أعمال التحقيق، ويتضمن مساساً بالحياة الخاصة التي كفلها الدستور والقوانين، ومنها قانون الإجراءات الجزائية.

ولا يعني ما سبق عدم أهمية إجراءات الاستدلالات في مواجهة جرائم الإنترنت والهاتف، فهي وإن كانت ليست من مراحل الدعوى الجزائية، إلا أنها تتيح لسلطة التحقيق أن تتصرف في الدعوى الجزائية وهي على بينة، من خلال الإجراءات الأولية التي باشرها مأمور الضبط القضائي، والتي منها استبعاد الدعاوى الكيدية وغير الجدية، وكذا تقييم أقوال الشهود بشأن الجريمة وكيفية ارتكابها، وغيرها من الأمور الفنية التي تساعد سلطة التحقيق في الوصول إلى الحقيقة[1].

---

[1] للمزيد أنظر: د. فتوح الشاذلي، عفيفي كامل عفيفي، جرائم الكمبيوتر، منشورات الحلبي الحقوقية، بيروت، لبنان، طبعة 2003، ص353، د. حسين سعيد الغافري، مرجع سابق، ص444.

ثانياً: الاختصاصات الاستثنائية لمأموري الضبط القضائي في مواجهة جرائم الإنترنت والهاتف:

من المعروف أن الاختصاصات الاستثنائية لمأموري الضبط القضائي تكون في حالة الجريمة المشهودة (التلبس)، وفي حالة الندب للتحقيق، وهذا ما أكده قانون الإجراءات الجزائية في المواد (99– 108، 117) وسوف نبين ذلك فيما يلي:

1 - اختصاص مأموري الضبط القاضي في جرائم الهاتف والإنترنت في حالة الجريمة المشهودة:

تناول المشرع حالات الجريمة المشهودة في عدة نصوص قانون الإجراءات الجزائية، إذ نصت المادة (99) منه على أنه: "في الجرائم المشهودة يتعين على مأمور الضبط القضائي أن ينتقل فوراً إلى محل الواقعة لمعاينة الآثار المادية للجريمة أو المحافظة عليها، وإثبات حالة الأماكن والأشخاص وكل ما يفيد في كشف الحقيقة، وسماع أقوال من كان حاضراً أو من يمكن الحصول منه على إيضاحات في شأن الواقعة ومرتكبيها، ويجب عليه فوراً أن يخطر النيابة العامة بانتقاله".

كما نصت المادة (101) منه على أنه: "في الجرائم المشهود المعاقب عليها بالحبس مدة لا تزيد على ستة أشهر يحق لمأمور الضبط القضائي القبض على كل شخص يستدل بالقرائن على أنه الفاعل للجريمة أو له علاقة بها إن كان حاضراً وأن يأمر بإحضاره إن كان غائباً".

ونصت المادة (102) منه أيضاً على أن: "لمأمور الضبط القضائي في الحالات المنصوص عليها في المادة السابقة أن يفتش المتهم ومنزله ويضبط الأشياء والأوراق التي تفيد في كشف الحقيقة متى وجدت أمارات قوية تدل على وجودها فيه".

وبالتأمل في هذه النصوص نجد أنها تتعلق بالإجراءات الواجب إتباعها في الجرائم التقليدية المشهودة، ولم تُشر إلى الجرائم المعلوماتية، ومع ذلك يمكن إعمال هذه النصوص لتستوعب الجرائم المعلوماتية – ومنها جرائم الإنترنت والهاتف

– وبهدف مواجهة الفراغ التشريعي، وبالتالي فإنه يجوز القبض على المتهم في الجرائم المعلوماتية والتفتيش في كل ما يتعلق بارتكاب هذه الجرائم[1].

ولكن الجرائم المشهودة في معظم الجرائم المعلوماتية من الصعب إثباتها في الأماكن الخاصة، كون القانون أحاطها بعدة ضمانات كونها مستودعاً لأسرار الأفراد ومقراً لأمنهم وخصوصياتهم التي لا يجوز للغير الإطلاع عليها، أما بالنسبة للأماكن والمحال العامة؛ كمقاهي الإنترنت وأماكن الاتصالات العامة فالأمر يختلف، إذ يجوز لمأمور الضبط القضائي ارتيادها كغيره من الناس، ولكن هذا الدخول لا يجيز له التفتيش للأجهزة المعلوماتية إلا في الأحوال المبينة في القانون، ومنها الجرائم المشهودة[2].

وتأسيساً على ما سبق، فإن جرائم الإنترنت والهاتف – كغيرها من الجرائم المعلوماتية – يمكن أن تكون محلاً لإجراءات مأمور الضبط القضائي في حالة الجريمة المشهودة – مع الصعوبة الكبيرة التي تكتنف هذه الجرائم – إذ يستطيع مأمور الضبط القضائي الذي يكتشف جريمة مشهودة على شبكة الإنترنت أثناء دخوله المحال العامة؛ كمقاهي الإنترنت أن يقوم بالقبض على صاحبها وتفتيش جهاز الكمبيوتر الذي استخدمه المتهم لارتكاب جريمته بواسطته وأخذ أقوال الشهود الموجودين لإثبات ذلك على المتهم، ومع ذلك تثير هذه الإجراءات الشك بشأن مدى صحتها، لاسيما مع وجود نص المادة (100 أ.ج) التي لا تجيز القبض والتفتيش إلا في حالة الجريمة المشهودة الجسيمة، وجرائم الإنترنت لا يوجد نصوص قانونية تحدد مدى جسامتها.

أما بالنسبة لجرائم الهاتف فمن الصعب إثبات الجريمة المشهودة فيها، لاسيما عند دخول مأمور الضبط القضائي إلى أحد المحال العامة المخصصة للاتصالات، فقد يصل إلى سمعه جريمة مشهودة أثناء مكالمة هاتفية يقوم بها أحد

---

(1) د. طارق إبراهيم الدسوقي عطية, الأمن المعلوماتي, دار الجامعة الجديدة للنشر, الإسكندرية, طبعة 2009, ص437.

(2) د. فتوح الشاذلي, عفيفي كامل عفيفي, مرجع سابق, ص360 وما بعدها.

مرتادي هذه المحال العامة، لكن من الصعب عليه إثبات ارتكاب الجريمة من خلال سماعه للمكالمة، إذ يصعب عليه تسجيل المكالمة أو ضبط أي دليل يُثبت نسبة الجريمة إلى المتهم، لكن يمكن أن يكتشف مأمور الضبط القضائي جريمة مشهودة تستخدم بواسطة الهاتف المحمول للشخص أثناء وجوده في محل عام، سواء بواسطة الرسائل أو ارتياد المواقع المشبوهة في الإنترنت، فهذه الحالة تثير اشكالية حول مدى صلاحية مأمور الضبط القضائي لاتخاذ إجراءات الجريمة المشهودة، خاصة أن أداة الجريمة – الهاتف – هي من الوسائل التي كفل لها القانون حماية خاصة[1]، ولا توجد نصوص واضحة في قانون الإجراءات الجزائية، وقانون الجرائم والعقوبات تصنف هذه الجرائم من حيث مدى جسامتها وتضع لها العقوبة المناسبة لها، إذ أن إجراءات القبض والتفتيش في حالة الجريمة المشهودة لا يستطيع مأمور الضبط القضائي مباشرتها إلا في حالة الجريمة المشهودة الجسيمة حسب نص المادة (100 أ.ج)

2 - **اختصاصات مأمور الضبط القضائي في حالة الندب من النيابة العامة:**

نصت المادة (117 أ.ج) على أن: "لعضو النيابة العامة أن يندب أحد مأموري الضبط القضائي للقيام بعمل أو أكثر من أعمال التحقيق عدا استجواب المتهم.."، وهذا النص وإن كان ينطبق على الجرائم التقليدية، إلا أنه يمكن إعماله في جرائم الإنترنت والهاتف – كغيرها من جرائم المعلومات – حتى لا يكون هناك جرائم دون عقاب.

وتأسيساً على ذلك، فإن مأمور الضبط القضائي وإن كان لا يملك أي اختصاص أصيل في أعمال التحقيق، إلا أنه يجوز لسلطة التحقيق ندبه لمباشرة بعض إجراءات التحقيق – فيما عدا الاستجواب – مع مراعاة الضمانات التي تطلبها القانون[2].

---

(1) نص المادة (2/12) من قانون الإجراءات الجزائية.

(2) بشأن هذا الموضوع أنظر: د. سعيد عبداللطيف حسن, مرجع سابق, ص224.

وتطبيقاً لما سبق، فإن مأمور الضبط القضائي يستطيع – بناءً على الندب – القيام ببعض أعمال التحقيق في جرائم الإنترنت والهاتف.

وللمزيد من البيان بشأن هذا الموضوع، فإننا سوف نتناول هذه الجرائم على النحو الآتي:

أ. جرائم الإنترنت:

أصبحت شبكة الإنترنت – كشبكة معلومات عالمية – وسيلة لارتكاب جرائم كثيرة، لذلك فإن مأمور الضبط القضائي – بناء على الندب – يملك بعض أعمال التحقيق لتفتيش أجهزة الحاسوب للبحث عن الأدلة حول الجرائم المرتكبة بواسطة الإنترنت في حدود القيود الخاصة بالندب[1].

ولكن تبدو الصعوبة في كون التفتيش في جرائم الإنترنت – كغيرها من الجرائم المعلوماتية – يتطلب المعرفة بالأنظمة والبرامج المعلوماتية، التي تتجاوز الثقافة العامة والمعرفة السطحية لهذه الأمور، إذ يتطلب الأمر معرفة كبيرة بكيفية التعامل مع برامج وملفات البيانات المخزنة آلياً، وكلمة المرور للدخول إلى النظام، وكيفية تتبع خيوط الجريمة وموقع الجاني وغير ذلك من الأمور الفنية، وهذا ما يفتقده معظم مأموري الضبط القضائي. ويزداد الأمر صعوبة وتعقيداً أن القانون لم يُجز إجبار المتهم على البوح بأية بيانات تؤدي إلى إدانته، ومن هذه البيانات كلمة المرور للجهاز الذي استخدمه المتهم لارتكاب إحدى جرائم الإنترنت[2].

ولمعالجة مشكلة عدم معرفة مأموري الضبط القضائي أثناء القيام بعمل التفتيش عن جرائم الإنترنت في جهاز الحاسوب بموجب أمر الندب من النيابة، فإنه يجب عليه مراعاة الآتي[3]:

---

(1) د. طارق إبراهيم الدسوقي عطية، مرجع سابق، ص430.

(2) د. فتوح الشاذلي، عفيفي كامل عفيفي، مرجع سابق، ص365.

(3) المهندس/ حسن طاهر داوود، جرائم أنظمة المعلومات، أكاديمية نايف للعلوم الأمنية، الرياض، الطبعة الأولى، 2000م، ص223.

- عدم إدخال أي تعديل على الوضع الذي يجد عليه الحاسوب حتى حضور النيابة والمختص.
- عدم السماح للمتهم باستخدام جهاز الحاسوب أو الدخول إلي شبكة الانترنت حتى لا يؤدي ذلك إلى ضياع الأدلة.

كما أنه يمكن لمأمور الضبط القضائي المنتدب التفتيش في شبكة الإنترنت، من خلال تتبع مرتكب الجرائم عبر الإنترنت بالاستعانة بمزود خدمات الإنترنت الرئيسي أو الفرعي (Service Provider)، إذ يمكن اختراق خصوصيات مستخدم الإنترنت، واكتشاف كل أفعاله عندما يتصل بالشبكة، ويشمل ذلك عناوين المواقع التي زارها ووقتها، والصفحات التي أطلع عليها، والرسائل التي أرسلها أو المواقع التي أخترقها، والحوارات التي شارك فيها، والخدمات التي اشترك فيها، وغير ذلك من الأعمال التي خالف بها القانون؛ فعندما يتجول مستخدم الإنترنت يترك آثاراً تدل عليه، ويمكن استخدامها كقرائن على قيامه بأعمال مخلة بالقانون، كما أن الأنظمة البرمجية المستخدمة في الإنترنت يمكن أن تسهل عملية البحث في شبكة الإنترنت والوصول إلى التفصيلات البرمجية؛ مثل برنامج (Proksey)، وكذا برنامج العناوين البريدية (Address) في شبكة الإنترنت، حيث يمكن من خلالها الحصول على عنوان البريد الإلكتروني للمستخدم واسمه الحقيقي [1].

ب. جرائم الهاتف:

أحاط القانون الحياة الخاصة بالحماية، فلا يجوز المساس بها وفقاً للقانون، إذ نصت المادة (2 أ.ج) على أن: "حرية وسرية المراسلات البريدية والسلكية واللاسلكية وكافة وسائل الاتصال مكفولة وفقاً للدستور ولا يجوز مراقبتها أو تفتيشها أو إفشاء سريتها أو تأخيرها أو مصادرتها إلا في الحالات التي يبينها القانون، وبأمر من النيابة العامة أو من المحكمة المختصة".

---

(1) د. ممدوح عبدالحميد عبدالمطلب, البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت, دار الكتب القانونية, القاهرة, طبعة 2006م, ص 67 وما بعدها.

كما أكدت المادة (14) – سالفة الذكر – من القانون ذاته على عدم جواز المساس بحرية الحياة الخاصة للمواطن في غير الأحوال المصرح بها في هذا القانون.

وتطبيقاً لما سبق، فإنه ليس لمأمور الضبط القضائي أي اختصاص أصيل في جرائم الهاتف، نظراً للحماية التي كفلها القانون لوسائل الاتصالات السلكية واللاسلكية، لأنها تدخل في عداد الحياة الخاصة للشخص، لذلك لا يجوز استراق السمع والتنصت على الأحاديث الخاصة وتسجيلها أو الإطلاع على الرسائل، لأن ذلك يمثل اعتداءً صارخاً على الحياة الخاصة، إلا أن مصلحة التحقيق قد تتطلب اللجوء إلى مراقبة وتسجيل الأحاديث الخاصة وفق الضوابط القانونية[1].

ولا يشترط أن يقوم بها عضو النيابة فقد يندب مأمور الضبط القضائي أو أحد رجال الهاتف للقيام بهذه الأعمال أو بعضها، وهذا ما أشارت إليه المواد (117، 132، 146)، من قانون الإجراءات الجزائية اليمني.

وتأسيساً على ذلك، يستطيع مأمور الضبط القضائي – بناءً على أمر الندب – القيام بالإجراءات المتعلقة بمراقبة وتسجيل المحادثات السلكية واللاسلكية أو الشخصية، وكذا ضبط الأشياء التي تفيد في التحقيق وإثبات التهمة على المتهم، وهذا ما أكدته المادة (132 أ.ج)، إذ نصت على أنه: "لا يجوز تفتيش الأشخاص أو دخول المساكن أو الإطلاع على المراسلات البريدية أو تسجيل المحادثات السلكية واللاسلكية أو الشخصية، وكذا ضبط الأشياء إلا بأمر من النيابة العامة أثناء التحقيق ومن القاضي أثناء المحاكمة".

وفي هذا النص نجد أن المشرع اليمني كان أكثر تنظيماً في هذا المجال من المشرع المصري، إذ أن المشرع في قانون الإجراءات الجنائية المصري لم يسمح في المادة (206) منه للمحقق سلطة تسجيل المكالمات، وإنما فقط تفريغ المكالمة في محضر رسمي، وهذا قد يعيب المحضر ويجعله عرضة للطعن أثناء المحاكمة.

---

(1) د. عبدالفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، مرجع سابق، ص374.

والتساؤل الذي قد يطرح هنا هو: هل يجوز ندب مأموري الضبط القضائي من قبل النيابة العامة للقيام بمراقبة المحادثات السلكية واللاسلكية؟

الحقيقة أن ذلك جائز ولا يوجد ما يمنع ذلك قانوناً، لأن هذا الإجراء شأنه شأن بقية إجراءات التحقيق – ما عدا الاستجواب – يجوز الندب فيها، شرط أن تتوافر بقية الشروط اللازمة للندب[1].

كما أنه من حق النيابة العامة أن تُكلف أحد رجال الهاتف بالاستماع إلى المحادثات الهاتفية وتسجيلها لنقل مضمونها إليه، وهذا ما أشارت إليه المادة (146) من قانون الاجراءات الجزائية اليمني، إذ نصت على أنه: ".. ويجوز بأمر من رئيس النيابة تكليف أحد رجال إدارة الهاتف بعد تحليفه اليمين القانونية بالاستماع إلى المحادثات الهاتفية وتسجيلها لنقل مضمونها إليه، ويجب أن يتضمن الأمر تحديداً واضحاً ودقيقاً للمكالمة المطلوب تسجيلها في خلال مدة 30 يوماً من تاريخ صدور الأمر.

[1] المرجع السابق، ص376.

المطلب الثاني
الشروط والقواعد الواجب مراعاتها أثناء مباشرة إجراءات الاستدلال في جرائم الإنترنت والهاتف

الدليل الرقمي كغيره من الأدلة الأخرى، يتطلب للحصول عليه وجود عدد من الشروط ومراعاة مجموعة من القواعد العامة، وعدم مراعاتها يجعل الدليل باطلاً، ويترتب على ذلك بطلان الآثار المترتبة عليه، وهذا ما أشارت إليه المادة (396 أ.ج)، وفي ما يلي نبين هذه الشروط والقواعد، وذلك على النحو الآتي:

أولاً: الشروط الواجب مراعاتها أثناء إجراءات الاستدلال

جرائم الإنترنت والهاتف – كغيرها من الجرائم المعلوماتية – محاطة بالحماية القانونية، وهذا ما أشارت إليه المادة (2 أ.ج) بقولها: "حرية وسرية المراسلات البريدية واللاسلكية وكافة وسائل الاتصال مكفولة وفقاً للدستور، ولا يجوز مراقبتها أو تفتيشها أو إفشاء سريتها أو تأخيرها أو مصادرتها إلا في الحالات التي يبينها القانون.."، لذلك يجب توافر عدد من الشروط أثناء إجراءات الاستدلال في جرائم الإنترنت والهاتف وغيرها من الجرائم المعلوماتية، وتتمثل هذه الشروط في الآتي:

1 - **وقوع جريمة معلوماتية:**

مع عدم وجود نصوص صريحة في جرائم الإنترنت والهاتف، إلا أن الجرائم المعلوماتية، ومنها جرائم الإنترنت والهاتف تستدعي تدخل مأمور الضبط القضائي لاتخاذ إجراءات الاستدلال حيالها، إذ أن نصوص قانون الإجراءات الجزائية هي نصوص عامة لم تحدد نوع معين من الجرائم، وهذا ما أكدته المادة (91 أ.ج) بقولها: "مأمورو الضبط القضائي مكلفون باستقصاء الجرائم وتعقب مرتكبيها..".

وتأسيساً على ذلك، فإن تدخل مأمور الضبط القضائي مشروط بوقوع جريمة من الجرائم المعلوماتية كغيرها من الجرائم التقليدية.

2- **توافر دلائل كافية على نسبة الجريمة المعلوماتية إلى المتهم:**

من البديهي أن مأمور الضبط القضائي لا يستطيع اتخاذ إجراءات الاستدلال أو بعض إجراءات التحقيق في الجرائم المشهودة أو في حالة الندب من النيابة المختصة حيال المتهم إلا إذا توفرت تجاهه الدلائل الكافية التي تؤكد نسبة

الجريمة إليه، وهذا ما أكدته عدد من نصوص قانون الإجراءات الجزائية، ومنها المواد (101، 102، 136، 137).

لذلك فإنه لابد أن تتوفر أسباب كافية على وجود أدوات استخدمت في الجريمة المعلوماتية أو آثار متحصلة منها أو مستندات الكترونية يحتمل أن يكون لها فائدة في ظهور الحقيقة ونسبتها إلى المتهم[1].

3- أن يكون محل التفتيش الأدوات المستخدمة في جرائم الإنترنت والهاتف:

لمأمور الضبط القضائي القيام بالتفتيش – في حالة الجريمة المشهودة أو في حالة الندب – في جرائم الإنترنت، ومن خلال تفتيش جهاز الحاسوب، أو من خلال مراقبة وتسجيل المحادثات الخاصة والإطلاع على الرسائل بناءً على ندب عضو النيابة المختص، فالدليل الرقمي هو الذي يحتوي بداخله مجموعة البيانات الرقمية التي تؤكد الإدانة أو البراءة، وهو بذلك ذو خصائص تختلف عن الأدلة التقليدية التي يمكن إزالة بعضها بسهولة، كبصمات الأصابع، أما الدليل الرقمي فإنه وإن كان من الممكن إزالته، إلا أنه توجد برمجيات – من ذات الطبيعة الرقمية – يمكن بمقتضاها استرداد كافة الملفات التي تم إزالتها[2].

4- كتابة المحاضر:

مع أن قانون الإجراءات الجزائية لم ينص على جرائم الإنترنت والهاتف، إلا أنه يجب على مأمور الضبط القضائي المختص إثبات إجراءات الاستدلال عن الجريمة المعلوماتية في المحضر، كغيرها من الجرائم التقليدية، وهذا ما أكدته المادة (91 أ.ج)[3].

---

(1) د.عبدالفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، مرجع سابق، ص388.

(2) للمزيد أنظر: د. حسين بن سعيد الغافري، مرجع سابق، ص535 وما بعدها.

(3) حيث نصت على أنه: "مأمور الضبط القضائي مكلفون باستقصاء الجرائم وتعقب مرتكبيها وفحص البلاغات والشكاوى وجمع الاستدلالات والمعلومات المتعلقة بها وإثباتها في محاضرهم..".

5- **حضور المتهم أو من يقوم مقامه:**

في حالة قيام مأمور الضبط القضائي بالتفتيش عن الدليل الرقمي في جرائم الإنترنت والهاتف – في الجريمة المشهودة وحالة الندب للتحقيق – فإنه ينبغي حضور المتهم أو من ينيبه وبحضور شاهدين من أقاربه أو جيرانه، وهذا ما أشارت إليه المادة (134 أ.ج).

ثانياً: القواعد العامة الواجب مراعاتها أثناء مباشرة إجراءات الاستدلال:

يجب على مأموري الضبط القضائي مراعاة مجموعة من القواعد العامة أثناء مباشرتهم لأعمال الضبط القضائي، أو أثناء القيام ببعض إجراءات التحقيق في الجرائم المشهودة أو في حالة الندب من عضو النيابة المختص، وتتمثل هذه القواعد في الآتي:

1- **الحصول على الدليل بصورة مشروعة:**

كفل الدستور اليمني صيانة الكرامة الإنسانية للمواطنين وحماية خصوصياتهم، لذلك نظم قانون الاجراءات الجزائية قواعد التعامل مع المتهمين، كالقبض والحبس والتفتيش والاستجواب وغيرها من الإجراءات، وهذا ما نصت عليه المادة (47) من دستور الجمهورية اليمنية، حيث نصت على أنه: "أ. تكفل الدولة للمواطنين حريتهم الشخصية وتحافظ على كرامتهم وأمنهم، ويحدد القانون الحالات التي تقيد فيها حرية المواطن، ولا يجوز تقييد حرية أحد إلا بحكم من محكمة مختصة.

ب. لا يجوز القبض على أي شخص أو تفتيشه أو حجزه إلا في حالة التلبس أو بأمر توجبه ضرورة التحقيق وصيانة الأمن يصدره القاضي أو النيابة العامة وفقاً لأحكام القانون".

ونصت المادة (52) منه على أن: "حرية وسرية المواصلات البريدية والهاتفية والبرقية وكافة وسائل الاتصال مكفولة، ولا يجوز مراقبتها أو تفتيشها أو إفشاء سريتها أو تأخيرها أو مصادرتها إلا في الحالات التي يبينها القانون وبأمر قضائي".

وتأسيساً على هذه النصوص، فإن إجراءات الحصول على الدليل يجب أن تكون مشروعة في إطار القواعد العامة التي حددها الدستور، وإلا فإن الدليل المستمد بطريق مخالف للأحكام الواردة في الدستور يكون باطلاً بطلاناً مطلقاً لتعلقه بالنظام العام.

ومن أمثلة الطرق غير المشروعة الحصول على الدليل بالإكراه المادي أو المعنوي للمتهم لإجباره على فك الشفرة أو بهدف الوصول إلى البيانات المخزنة آلياً، أو التنصت على المكالمات أو الاطلاع على الرسائل بدون وجه قانوني[1].

ومن أجل تحقق مشروعية الإجراءات أيضاً، فإنه يجب صدور الأوامر القضائية لمأموري الضبط القضائي في حالة الندب لمباشرة بعض إجراءات التحقيق[2].

2- **إمكانية مناقشة الدليل الإلكتروني المستخرج من الإنترنت والهاتف:**

وهذه القاعدة تعني أن القاضي لا يمكن أن يُكوّن قناعته من الدليل الإلكتروني ما لم يؤسس على مناقشة الدليل الإلكتروني المبني على العناصر الإثباتية التي طرحت في جلسات المحكمة من جميع أطراف الدعوى وبحرية كاملة، وهذا يعني أن جميع الأدلة الإلكترونية ستكون محلاً للمناقشة عند الأخذ بها كأدلة إثبات أمام المحكمة، وعلى ذلك فإن كل دليل يتم الحصول عليه من خلال بيئة تكنولوجيا المعلومات يجب أن يخضع للنقاش أمام القاضي، وكذلك الشهود وخبراء الأنظمة المعلوماتية يجب أن يخضعوا للمناقشة أمام القاضي[3]. وهذا ما أشارت إليه عدد من نصوص قانون الإجراءات الجزائية (224، 226، 234).

3- **أن تكون الأدلة الإلكترونية غير قابلة للشك:**

يجب أن يكون الدليل الإلكتروني – الذي يتم الحصول عليه من الإنترنت والهاتف عن جريمة ارتكبت – غير قابل للشك حتى يمكن الحكم بالإدانة، إذ أنه لا مجال لدحض قرينة البراءة وافتراض عكسها إلا إذا وصل اقتناع القاضي إلى حد الجزم واليقين، وأن يحدد قوتها الاستدلالية على صدق نسبة الجريمة المعلوماتية إلى شخص معين من عدمه[4].

---

(1) د.علي حسن الطوالبة، التفتيش الجنائي على نظام الحاسوب والإنترنت، عالم الكتب الحديث، الأردن، طبعة 2004م ص184 وما بعدها.

(2) د. حسين بن سعيد الغافري، مرجع سابق، ص528.

(3) د.علي حسن الطوالبة، مرجع سابق، ص193.

(4) المرجع السابق، ص190.

المبحث الثالث

الجزاء المترتب على مخالفة مأموري الضبط القضائي للقواعد الإجرائية

شددت معظم الدساتير على الحفاظ على خصوصيات الإنسان، لذلك وضع القانون مجموعة من القواعد الإجرائية التي تضمنت الحفاظ على هذا الأصل، وقد تضمن دستور الجمهورية اليمنية وقانون الإجراءات الجزائية نصوصاً تنظم القواعد الواجب إتباعها للحصول على الدليل، إذ نصت المادة (52) من الدستور على أن: "حرية وسرية المواصلات البريدية والهاتفية والبرقية مكفولة، ولا يجوز مراقبتها أو تفتيشها أو إفشاء سريتها أو تأخيرها أو مصادرتها إلا في الحالات التي يبينها القانون وبأمر قضائي".

وقد رتب قانون الاجراءات الجزائية اليمني البطلان كجزاء إجرائي على مخالفة القواعد الإجرائية التي حددها المشرع في هذا القانون. كما رتب قانون الجرائم والعقوبات العقوبة المناسبة على هذا العمل غير المشروع.

وتأسيساً على ذلك يجب على مأموري الضبط القضائي – كغيرهم من أجهزة العدالة – مراعاة هذه القواعد من أجل تحقيق مشروعية الإجراءات، وحتى لا يوصم الدليل بعدم المشروعية، لذلك فإننا في هذا المبحث سوف نتناول الجزاء المترتب على مخالفة مأموري الضبط القضائي للقواعد الإجرائية من خلال تقسيم هذا المبحث إلى مطلبين، وذلك على النحو الآتي:

المطلب الأول: الجزاء الاجرائي المترتب على مخالفة مأموري الضبط القضائي للقواعد الإجرائية (بطلان الدليل).

المطلب الثاني: الجزاء الجنائي والمدني المترتب على مخالفة مأموري الضبط القضائي للقواعد الإجرائية.

المطلب الأول

الجزاء الاجرائي المترتب على مخالفة مأموري الضبط القضائي للقواعد الإجرائية (بطلان الدليل)

من المسلم به أنه لا يجوز الاستناد في الإدانة على أدلة غير مشروعة جاءت ثمرة لانتهاك الحرية الشخصية، لأنه يشترط في دليل الإدانة أن يكون مشروعاً، إذ لا يجوز أن تبنى الإدانة على دليل باطل[1].

والبطلان هو: "جزاء إجرائي يرد على العمل الإجرائي المخالف لبعض أو كل القواعد الإجرائية فيهدر آثاره القانونية"[2].

لذلك فإن البطلان يترتب على مخالفة القواعد الإجرائية التي حددها المشرع، كجزاء إجرائي على العمل المخالف للقانون، وهذا ما قررته المادة (396 أ.ج) إذ نصت على أنه: "يقع باطلاً كل إجراء جاء مخالفاً لأحكام هذا القانون، إذا نص القانون صراحةً على بطلانه أو إذا كان الإجراء الذي خولف أو أغفل جوهرياً".

وتأسيساً على ما ورد في نص المادة (396 أ.ج) – السالفة الذكر – فإن البطلان يترتب إذا نص القانون صراحة على بطلان الإجراء المخالف، أو إذا كان الإجراء الذي خولف أو أغفل جوهرياً، وبمطالعة نص المادة (397 أ.ج) نجد أنها نصت صراحة على بعض الحالات التي يترتب عليها البطلان، إلا أنها لم تحدد المقصود بالعيب الإجرائي الجوهري، إذ نصت على أنه: "إذا كان البطلان راجعاً لعدم مراعاة أحكام القانون المتعلقة بكيفية رفع الدعوى الجزائية أو بتشكيل المحكمة أو بولايتها بالحكم في الدعوى أو بعلانية الجلسات أو تسبيب الأحكام أو حرية الدفاع أو علانية النطق بالأحكام أو إجراءات الطعن أو العيب الإجرائي الجوهري المهدر لأي حق من حقوق المتقاضيين فيها أو غير ذلك مما هو متعلق بالنظام العام.. ".

---

(1) د. سعيد عبداللطيف حسن، مرجع سابق، ص225.

(2) د.علي حسن الطوالبة، مرجع سابق، ص167.

وبما أن القانون الإجرائي لم يحدد المقصود بالعيب الإجرائي الجوهري، فقد ترك ذلك التحديد لاجتهاد الفقه والقضاء. والمقصود بالإجراء الجوهري في تفسير الفقه القانوني هو: ذلك الاجراء الذي يكون مقصوداً منه المحافظة على مصلحة المتهم أو أحد الخصوم[1].

ولتطبيق ما سبق على دور مأموري الضبط القضائي في جرائم الإنترنت والهاتف نجد أن مهامهم – كسلطة استدلال أو في حالة الندب للتحقيق – قد تطال المصلحة التي يحميها المشرع، وهي مصلحة المتهم أو أحد الخصوم، والتي نص على حمايتها قانون الإجراءات الجزائية في المادة (132) منه، والتي نصت على أنه: "لا يجوز تفتيش الأشخاص أو دخول المساكن أو الإطلاع على المراسلات البريدية أو تسجيل المحادثات السلكية أو اللاسلكية أو الشخصية وكذا ضبط الأشياء إلا بأمر من النيابة العامة أثناء التحقيق ومن القاضي أثناء المحاكمة".

ولمحكمة الموضوع أن تُكوّن قناعتها من أي دليل في الدعوى، فلها أن تأخذ بما جاء في محضر الاستدلال وأن تستمد منه قناعتها، وللمحكمة أن تراقب الدليل المأخوذ من سلطة الاستدلال من زاويتين[2]:

1 - **المشروعية**: فإذا خالفت سلطة الاستدلال الضمانات التي حددها القانون لحماية الحرية الشخصية أصبحت معيبة بالبطلان.

2 - **الموضوعية**: من خلال حرية الامتناع، فللمحكمة أن تطرح ما ورد في محضر الاستدلالات من معلومات إذا لم تطمئن إلى جديتها أو إلى مطابقتها للحقيقة.

ويبدو من سياق نص المادة (396 أ.ج) أن المشرع اتجه في تحديد العيب الإجرائي الجوهري إلى الأخذ بمذهب البطلان الذاتي، الذي يقرر أن الوسيلة لتقرير البطلان ليست تشريعية – كما هو في مذهب البطلان القانوني – وإنما

---

(1) محمد كامل إبراهيم, النظرية العامة للبطلان في قانون الإجراءات الجنائية, دار النهضة العربية, القاهرة, 1989م, ص39.

(2) د.عبدالحميد الشواربي, البطلان الجنائي, منشأة المعارف, الإسكندرية, لم يحدد تاريخ النشر, ص126.

الوسيلة إلى ذلك قضائية، بمعنى أن يترك للقاضي تقدير حالات البطلان في كل حالة على حده، ويضع المشرع عادةً معياراً مجرداً يستعين به القاضي في التمييز بين القواعد التي يترتب على مخالفتها البطلان، وتلك التي لا يبطل الاجراء لمخالفتها، وهذا المعيار يقوم على التفرقة بين القواعد الإجرائية الجوهرية؛ وهي التي تحمي مصالح أساسية، والقواعد غير الجوهرية؛ وهي التي تحمي مصالح أقل أهمية، والبطلان جزاء لمخالفة الأولى دون الثانية، أي أن البطلان في هذا المذهب انتقائي بحسب أهمية القاعدة الإجرائية[1].

وكذلك الحال بالنسبة لإجراءات التحقيق التي يقوم بها مأمور الضبط القضائي في جرائم الإنترنت والهاتف وغيرها من جرائم المعلومات فإنها قد يشوبها البطلان إذا باشرها دون الندب من النيابة أثناء التحقيق أو من القاضي أثناء المحاكمة، أو إذا كان ندبه لاتخاذ هذه الإجراءات قد شابه عيب يبطله، أو إذا ثبت أنه قام بالضبط أو المراقبة قبل صدور الندب أو قبل صدور الأمر القضائي[2].

(1) د.علي حسن الطوالبة, مرجع سابق, ص169.

(2) محمد كامل إبراهيم, مرجع سابق, ص136.

المطلب الثاني
الجزاء الجنائي والمدني المترتب على مخالفة مأموري الضبط القضائي للقواعد الإجرائية

قرر القانون الحماية الجنائية للحريات وحرمة الحياة الخاصة، ووضع لها الضمانات الكافية، وتتمثل تلك الحماية في تقرير الجزاء عما يترتب على الاجراء المخالف الذي باشره مأمور الضبط القضائي للمشروعية من نتائج، بالإضافة إلى تقرير التعويض لجبر الضرر الناتج عن الاجراء المخالف.

لذلك فإنني في هذا المطلب سأتناول الجزاء الجنائي والمدني المترتب على مخالفة مأموري الضبط القضائي للقواعد الإجرائية، وذلك على النحو الآتي:

أولاً: الجزاء الجنائي

إن الممارسات غير المشروعة التي يباشرها مأمور الضبط القضائي أثناء قيامه بالبحث عن دليل في جرائم الانترنت والهاتف تؤدي – إضافة إلى بطلان الدليل المتحصل عليه – إلى تقرير المسئولية الجنائية عليه، إذ رتب المشرع على هذا العمل غير المشروع عقوبة مناسبة، حيث نصت المادة (255) من قانون الجرائم والعقوبات على أنه:" يعاقب بالحبس مدة لا تزيد على سنة أو بالغرامة من فتح بغير حق خطاباً مرسلاً إلى الغير أو احتجز رسالة برقية أو هاتفية،.. ويقضى بالحبس مدة لا تزيد على سنتين أو بالغرامة إذا ارتكب الجريمة موظف عام اخلالاً بواجبات وظيفته " [1]. كما نصت المادة (256) من القانون ذاته على أنه: " يعاقب بالحبس مدة لا تزيد على سنة أو بالغرامة كل من اعتدى على حرمة الحياة الخاصة، وذلك بأن ارتكب أحد الأفعال الآتية في غير الأحوال المصرح بها قانوناً أو بغير رضاء المجنى عليه:

أ -استرق السمع أو سجل أو نقل عن طريق جهاز من الأجهزة أياً كان نوعه محادثات جرت في مكان خاص أو عن طريق الهاتف.

ب - التقط أو نقل بجهاز من الأجهزة أياً كان نوعه صورة شخص في مكان خاص.

---

[1] القرار الجمهوري رقم (12) لسنة 1994م بشأن قانون الجرائم والعقوبات.

ويعاقب بالحبس مدة لا تزيد عن ثلاث سنوات أو بالغرامة الموظف العام الذي يرتكب أحد الأفعال المبينة بهذه المادة اعتماداً على سلطة وظيفته ".

وفي ذات المضمون نجد أن قانون الإمارات العربي الاسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها، المعتمد من مجلس وزراء العدل العرب بتاريخ 2003/10/3م قد نص في المادة الخامسة منه على عقوبة الحبس أو الغرامة على الموظف العام الذي دخل بغير وجه حق موقعاً أو نظاماً معلوماتياً، وفي ذات السياق نصت المادة (39) من وثيقة الرياض للنظام الموحد لمكافحة جرائم تقنية المعلومات لدول مجلس التعاون لدول الخليج العربي الصادرة 2013م.

وبمطالعة نصوص قانون الجرائم والعقوبات نجد أنه لم ينص صراحةً على الجرائم المعلوماتية، ولكنه أوجب عقوبة الحبس أو الغرامة على كل من انتهك حرمة الحياة الخاصة، وشدد العقوبة على من باشر الاجراء المخالف من الموظفين العامين – ومنهم مأموري الضبط القضائي – والسبب في تشديد العقوبة يرجع إلى ما يتمتع به مأمورو الضبط القضائي من سلطات، وإخلالهم بواجبات الوظيفة العامة، وكون ذلك أيضاً يمثل اعتداء على حرمة الحياة الخاصة التي يحيطها المشرع بالحماية الجنائية ([1]).

وبالنظر إلى مشروع تعديل قانون الجرائم والعقوبات المرفوع من وزير العدل إلى مجلس النواب بتاريخ 2010/4/7م نجد أنه لم يُدخل ضمن النصوص المقترح تعديلها أو المطلوب اضافتها ما يُشير إلى الجرائم المعلوماتية.

وتأسيساً على ما سبق، فإن الانتهاكات التي يمارسها مأمورو الضبط القضائي – كغيرهم من رجال السلطة العامة – يمكن أن تُبطل الدليل المتحصل عليه من هذه الوسائل، بالإضافة إلى تقرير المسئولية الجنائية على من قام بهذه الانتهاكات ([2]).

---

(1) بشأن هذا الموضوع أنظر: د. عادل إبراهيم صفا، سلطات مأموري الضبط القضائي بين الفعالية وضمان الحريات والحقوق الفردية، دار النهضة العربية، القاهرة، الطبعة الأولى 2009م، ص 451 وما بعدها.

(2) للمزيد بشأن هذا الموضوع أنظر: د. عماد مجدي عبد الملك، جرائم الكمبيوتر والانترنت، دار المطبوعات الجامعية، الاسكندرية، 2011م، ص 253.

ثانياً: الجزاء المدني

المسئولية المدنية عن أعمال مأموري الضبط القضائي ناتجة عن الخطأ، فمتى ثبت وقوع خطأ من مأمور الضبط القضائي أثناء تأدية وظيفته أو بسببها، فإن الإدارة تصبح مسئولة عن هذا الخطأ بطريق التضامن، ولا يمكنها أن تتخلص من المسئولية بزعم أنها لم تُقصر في واجب التوجيه والرقابة، وهذا ما أشارت إليه المادة (313) من القانون المدني اليمني، التي نصت على أنه: " يكون المتبوع مسئولاً عن الضرر الذي يحدثه تابعه بعمل غير مشروع أمره به، فإن عمل التابع عملاً غير مشروع أضر بالغير ولم يأمره المتبوع كانت المسئولية على التابع، وعلى المتبوع أن يُحظر العامل لتعويض الضرر الذي أحدثه " [1].

ويشترط لقيام مسئولية الإدارة عن أخطأ تابعيها توافر ثلاثة أركان[2]:

1. ركن الخطأ: ويتمثل في وقوع خطأ من مأمور الضبط القضائي أثناء تأدية وظيفته أو بسببها.
2. ركن الضرر: وهو الأذى المادي أو المعنوي الذي يلحق صاحب الشأن.
3. علاقة السببية بين الخطأ والضرر.

ويدخل في معنى الخطأ الذي تتوفر معه المسئولية العمل غير المشروع المخالف للقوانين واللوائح، والانحراف في استعمال السلطة[3].

وتأسيساً على ما جاء في نص المادة (313) من القانون المدني اليمني – سالفة الذكر – فإن الإدارة تكون مسئولة عن أعمال مأموري الضبط القضائي إذا أتى بعمل غير مشروع مخالفاً للقوانين واللوائح، وأضر بالغير، بشرط أن تكون هي من أمرته للقيام بهذا العمل، أما إذا قام بالعمل غير المشروع بدون الرجوع إلى إدارته، فإنه يتحمل المسئولية الشخصية بتعويض المضرور عما أصابه من ضرر، وليس على الإدارة سوى احضاره وإلزامه بتعويض الضرر.

---

[1] القانون رقم (14) لسنة 2002م بشأن القانون المدني.

[2] د. عادل إبراهيم صفا، مرجع سابق، ص 480.

[3] د. سعد عصفور، محسن خليل، القضاء الإداري، منشأة المعارف، الاسكندرية، 1964م، ص 528. ((مشاراً إليه في كتاب د. عادل إبراهيم صفا، مرجع سابق، ص 480)).

وفي الحالة التي تكون فيها الإدارة مسئولة عن تعويض الضرر الذي سببه مأمور الضبط القضائي للغير، فإنه يحق لها الرجوع عليه بعد ذلك لتسديد قيمة التعويض الذي قامت بتسليمه لجبر الضرر، وذلك في الحدود التي يكون فيها الغير مسئولاً عن تعويض الضرر[1].

وإعمالاً لما سبق، فإن قيام مأمور الضبط القضائي بأعمال غير مشروعة قانوناً – أثناء بحثه عن أدلة في جرائم ارتكبت بواسطة الانترنت والهاتف – يستلزم التعويض عن الضرر الذي سببه الاجراء غير المشروع الذي قام به، بالإضافة إلى الجزاءات الأخرى المقررة قانوناً.

وتجدر الاشارة إلى أن الحكم بالبراءة في الدعوى الجزائية المقامة ضد مأمور الضبط القضائي لا يتعارض مع إمكان الحكم بالتعويض عن الضرر الذي لحق بالمضرور نتيجة العمل غير المشروع الذي باشره مأمور الضبط القضائي، ولكن يشترط لذلك ما يلي[2]:

1. ثبوت وقوع الفعل موضوع الدعوى الجزائية وصحة اسناده إلى مأمور الضبط القضائي.
2. أن يكون الحق المدعى به ناشئاً عنه ضرر للمدعي من الجريمة المرفوعة بها الدعوى.

كما تجدر الاشارة أيضاً إلى أن عبء اثبات المسئولية عن العمل غير المشروع الذي صدر من مأمور الضبط القضائي يقع على عاتق المضرور، إذ أن المبادئ العامة في نظرية الاثبات تُقرر أن الأصل براءة الذمة، وأثره إلزام من يدعي على غيره حقاً أو قولاً بإثبات ذلك[3].

---

[1] إذ قضت المادة (314) من القانون المدني رقم (14) لسنة 2002م بأنه: " للمسئول عن عمل الغير حق الرجوع عليه في الحدود التي يكون فيها الغير مسئولاً عن تعويض الضرر ".

[2] د. عماد محمود أبو سمره، المسئولية المدنية لمأمور الضبط القضائي، دار الفكر والقانون، المنصورة، القاهرة، 2012م، ص 228.

[3] المرجع السابق، ص 182.

الخاتمة

حاولت في هذا البحث توضيح ما تتصف به جرائم الانترنت والهاتف – كغيرها من الجرائم المعلوماتية – من خصوصية تختلف بها عن غيرها من الجرائم التقليدية، وما تتطلبه من خبرات فنية في مأموري الضبط القضائي لاكتشافها وضبطها.

كما بينت مسئولية مأموري الضبط القضائي في جرائم الانترنت والهاتف، والتحديات التي تواجهه في هذا الصدد.

وقد قمت بدراسة هذا الموضوع الهام من خلال خطة أسأل الله تعالى أن أكون قد وفقت في إعدادها، وأن تكون قد حققت الغرض المرجو من هذا البحث، وفي الأخير أوردت مجموعة من النتائج والتوصيات أبينها على النحو الآتي:

أولاً: النتائج

أسفر البحث عن النتائج الآتية:

1. يوجد قصور في قانون الاجراءات الجزائية وقانون العقوبات في مجال تنظيم الجرائم المعلوماتية، مما ترتب عليه بعض الغموض وعدم وضوح الاجراءات اللازم اتباعها في مرحلة الاستدلالات في جرائم الانترنت والهاتف.
2. تختلف المعاينة في جرائم الانترنت والهاتف عن المعاينة في الجرائم التقليدية، فالأخيرة لا تتطلب سوى الانتقال إلى مسرح الجريمة لمعاينة أدلة الجريمة، بينما المعاينة للبحث عن الدليل الرقمي في جرائم الانترنت والهاتف تتطلب البحث في جهاز الحاسوب والهاتف، وهذا يُعد عمل من أعمال التفتيش الذي تختص به النيابة العامة.
3. تضع جرائم الانترنت والهاتف أجهزة الشرطة العاملة في مجال الضبطية القضائية أمام تحديات كبيرة لمواجهتها، لعدم توفر الإلمام الكافي والخبرات الفنية لدى مأموري الضبط القضائي بوسائل مواجهتها، بينما

تتطور وسائل ارتكاب هذه الجرائم يوماً بعد يوم بصورة أسرع من استجابة مأموري الضبط القضائي.

4. اقتصار المادة (84) من قانون الاجراءات الجزائية على تحديد صفة الضبطية القضائية في رتبة الضابط يؤثر سلباً اليوم على كفاءة جمع الاستدلالات بسبب أن معظم العاملين في مجال الدليل الرقمي من الأفراد والفنيين.

5. افتقار الشرطة إلى جهاز مختص في مجال الأدلة الرقمية يحد من قدرة مأموري الضبط القضائي في مواجهة الجرائم المعلوماتية.

6. خلو مناهج أكاديمية الشرطة من مادة الجرائم المعلوماتية يُعيق بناء قدرات مأموري الضبط القضائي في مواجهة الجرائم المعلوماتية.

ثانياً: التوصيات

في نهاية هذا البحث فإنني أوصي بما يلي:

1. ضرورة تعديل نص المواد (91، 92) من قانون الاجراءات الجزائية بإضافة وتحديد أعمال الاستدلالات والمعاينة في الجرائم المعلوماتية – ومنها جرائم الانترنت والهاتف – والتي تدخل في اختصاص الضبطية القضائية، لما لها من خصوصية تتعلق بالحريات الشخصية، وأرى الاستعانة بالخبراء والمختصين في المجال المعلوماتي لتحديد ما يمكن الاطلاع عليه من البيانات، والتي يمكن اعتبارها من إجراءات الاستدلال، وما يُعد منها من إجراءات التحقيق، وحتى لا يحدث انتهاكات للحقوق والحريات الخاصة، أو التداخل في الاختصاصات بين النيابة العامة وأجهزة الشرطة العاملة في مجال الضبطية القضائية.

2. ضرورة تأهيل مأموري الضبط القضائي في مجال التعامل مع الأدلة الرقمية، كما أنه من الضرورة بمكان تأهيل بقية أجهزة العدالة الأخرى – النيابة والقضاء – في مجال الأدلة الرقمية حتى لا يحدث قصور في اثبات الجريمة

على الجاني في أي مرحلة من مراحل الدعوى الجزائية.

3. ضرورة تدخل المشرع الاجرائي لمنح صفة الضبطية القضائية – فيما يتعلق بالجرائم المعلوماتية – للعاملين في مجال الأدلة الرقمية، الذين يصدر بتحديدهم قرار من السلطة المختصة، وعدم اقتصار ذلك على من يحملون رتبة ضابط، عملاً بما جاء في نص المادة (47) من القانون العربي الاسترشادي للمعاملات والتجارة الالكترونية الصادر في 2009/11/19م، وكذا نص المادة (41) من القانون العربي الاسترشادي للإثبات بالتقنيات الحديثة الصادر في2008/11/27م، ونص المادة (39) من وثيقة الرياض للنظام الموحد لمكافحة جرائم تقنية المعلومات لدول مجلس التعاون لدول الخليج العربي الصادرة 2013م.

4. ضرورة إنشاء معمل متكامل في مقر الإدارة العامة للأدلة الجنائية ليكون بيت خبرة لجميع الأجهزة الأمنية العاملة في مجال الضبطية القضائية، مع انشاء معمل مصغر في كلية الشرطة وآخر في كلية التدريب، للتدريب العملي على كيفية التعامل مع الدليل الرقمي.

5. ضرورة إدخال مادة الجرائم المعلوماتية كمادة أساسية وهامة في مناهج أكاديمية الشرطة لبناء القدرات الفنية لمأموري الضبط القضائي في مجال الدليل الرقمي.

6. ضرورة تفعيل التعاون العربي والدولي في مجال مكافحة الجرائم المعلوماتية، والاستفادة من خبراتهم في هذا المجال.

المراجع

أولاً: المراجع المتخصصة

1. المهندس/ حسن طاهر داوود، جرائم أنظمة المعلومات، أكاديمية نايف للعلوم الأمنية، الرياض، الطبعة الأولى، 2000م، ص223.
2. د. حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الإنترنت، دار النهضة العربية، القاهرة، طبعة 2009م.
3. د. سعيد عبداللطيف حسن، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت، دار النهضة العربية، القاهرة، الطبعة الأولى، عام 1999م.
4. د. طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي، دار الجامعة الجديدة للنشر، الإسكندرية، طبعة 2009م.
5. د. عادل إبراهيم صفا، سلطات مأموري الضبط القضائي بين الفعالية وضمان الحريات والحقوق الفردية، دار النهضة العربية، القاهرة، الطبعة الأولى 2009م.
6. د. عبدالحميد الشواربي، البطلان الجنائي، منشأة المعارف، الإسكندرية، لم يحدد تاريخ النشر.
7. د. عبدالفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، لم يحدد مكان النشر، طبعة 2009م.
8. د. عبدالفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، مصر، طبعة 2007م.
9. عبدالله عبدالكريم عبدالله، جرائم المعلوماتية والإنترنت، منشورات الحلبي الحقوقية، بيروت، لبنان، الطبعة الأولى 2007م.
10. د. علي حسن الطوالبة، التفتيش الجنائي على نظام الحاسوب والإنترنت، عالم الكتب الحديث، الأردن، طبعة 2004م.

11. د. عماد مجدي عبد الملك، جرائم الكمبيوتر والانترنت، دار المطبوعات الجامعية، الاسكندرية، 2011م.
12. د. عماد محمود أبو سمره، المسئولية المدنية لمأمور الضبط القضائي، دار الفكر والقانون، المنصورة، القاهرة، 2012م.
13. د. فتوح الشاذلي، عفيفي كامل عفيفي، جرائم الكمبيوتر، منشورات الحلبي الحقوقية، بيروت، لبنان، طبعة 2003م.
14. محمد علي العريان، الجرائم الإلكترونية، دار الجامعة الجديدة للنشر، الإسكندرية، طبعة 2004م.
15. محمد كامل إبراهيم، النظرية العامة للبطلان في قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، 1989م.
16. د. ممدوح عبدالحميد عبدالمطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، القاهرة، طبعة 2006م.
17. د. هدى حامد قشقوش، جرائم الحاسب الإلكتروني، دار النهضة العربية، القاهرة، طبعة 1992م.

ثانياً: التشريعات

1. دستور الجمهورية اليمنية.
2. القانون رقم (14) لسنة 2002م بشأن القانون المدني.
3. القرار الجمهوري رقم (12) لسنة 1994م بشأن قانون الجرائم والعقوبات.
4. القرار الجمهوري رقم (13) لسنة 1994م بشأن قانون الاجراءات الجزائية.