فعالية الأنظمة السعودية ذات الصلة في الحد من الجرائم المعلوماتية

الدكتـــــور
مشعل عبدالله العصيمى
رئيس قسم القانون بكلية العلوم والدراسات الإنسانية
بالدوادمى، جامعة شقراء المملكة العربية السعودية

ملخص البحث

نظراً لازدياد مستخدمي الإنترنت في المملكة العربية السعودية ، طبقاً لأخر التقارير الصادرة من هيئة الاتصالات وتقنية المعلومات وما يستتبع ذلك من تنامي خطر تهديد الجرائم المعلوماتية ،وما يترتب على ذلك من خسائر مالية كبيرة كأثر سلبي ناتج عن ارتكاب الجرائم المعلوماتية.

ومن ثم حاول الباحث التصدي للأنظمة القانونية المطبقة في المملكة العربية السعودية ومحاولة الوقوف على بعض الأنظمة القانونية المقارنة الأخرى وصولاً إلى معرفة مدى نجاعة ما سن من تشريعات لمواجهة هذا الخطر الذي تنوعت آثاره على المجتمع السعودي نظراً لتعدد صور وأشكال الجرم المرتكب.

تمهيد :

- أهمية موضوع البحث

تنبع أهمية موضوع البحث في عدة نقاط منها:

1- ما يترتب على الجرائم المعلوماتية من خسائر مالية في المملكة العربية السعودية ،بلغت أكثر من 2،6 مليار ريال سعودي طبقا لآخر إحصائيات شركة (سمانتك) [1].(صحيفة الاقتصادية العدد(7360) صفر 1435هـ).

2- ازدياد نسبة مستخدمي الانترنت في المملكة العربية السعودية خلال السنين الأخيرة حيث قفزت النسبة من 5% عام 2001 إلى 55% من إجمالي السكان بنهاية 2013م حيث وصل عدد المستخدمين إلى 16،5مليون. (التقرير السنوي لهيئة الاتصالات وتقنية المعلومات في المملكة العربية السعودية للعام1434/1435هـ(2013)،ص72).

3-أهمية وضرورة التوعية لمستخدمي الإنترنت من خطورة هذا النوع من الجرائم لاسيما وأن هناك شرائح مختلفة في أمس الحاجة إلى التوعية .

4- تهاون فئة كبيرة من مستخدمي الإنترنت من إتباع وسائل الحماية اللازمة كالحفاظ على سرية (كلمة المرور للبريد الإلكتروني) أو عدم الحفاظ على سرية المعلومات الشخصية عبر الشبكة العالمية.

- مشكلة البحث

تتلخص في مدى فعالية الأنظمة السعودية كنظام الجرائم المعلوماتية 1428هـ وبعض الأنظمة القانونية الأخرى في الحد والتقليل من الآثار الناجمة عن الجرائم المعلوماتية في المملكة العربية السعودية.

- فرضيات البحث

---

١) هي شركة عالمية تأسست عام 1982م لبيع برامج الكمبيوتر وخصوصا في مجال الأمن وإدارة المعلومات،يقع مركزها في كبيرتي نو بكاليفورنيا وتعمل في أكثر من 40 دولة.

1- كفاءة الأنظمة في الحد من درء الآثار السالبة نتيجة لارتكاب الجرائم المعلوماتية في المملكة العربية السعودية.
2- عدم ملائمة الأنظمة المطبقة في الحد من الجرائم المعلوماتية.

- منهج البحث

المنهج الوصفي:وذلك بوصف النصوص النظامية المعنية بالجرائم الالكترونية في المملكة العربية السعودية باعتباره منهج عام يمكن أن يعرف الجرائم المعلوماتية ويحدد أبعادها
المنهج المقارن :وذلك بمقارنة النصوص النظامية المطبقة في المملكة العربية السعودية فيما يخص الجرائم المعلوماتية مع نظيراتها في بعض الدول ؛ وذلك للتحقق من مدى ملائمة وتطور الأنظمة السعودية في هذا الصدد.

- أهداف البحث

وهما ينقسمان إلى نوعين الأول علمي يتعلق بإثراء المعرفة وإشباع النهم العلمي لدى الباحثين في هذا الحقل القانوني ،أما الثاني فهو عملي يبرز في الأتي:
1- صياغة نظام يعنى بالحد من الآثار الضارة الناجمة عن الجرائم المعلوماتية في سقفها الأعلى وذلك بالتغلب على كل ما يحول أو يعقد من صعوبة إثبات الجرائم المعلوماتية.
2- التأكيد على ضرورة المراجعة والمواكبة المستمرة متى ما استدعى الأمر ذلك فيما يتعلق بالصياغة التنظيمية لنظام مكافحة الجرائم المعلوماتية، والأنظمة السعودية ذات الصلة لمواجهة التنامي المستمر والمضطرد لهذه الجرائم.

خطة البحث

يهتم البحث بدراسة فعالية الأنظمة السعودية ذات الصلة في الحد من آثار الجرائم المعلوماتية ، لذا كان لابد أن يقسم البحث إلى مبحثين الأول منهما يعنى ببيان المفهوم العام للجرائم المعلوماتية لدى كتاب القانون بالإضافة إلى الأنظمة من حيث الآثار الضارة المترتبة عليها والأشكال والصور ...الخ. أما الثاني فهو يركز على الجانب الخاص بالأنظمة السعودية والمقارنة المعنية بالجرائم المعلوماتية وذلك بغرض التحقق من الفرضيتين التي أشرنا إليها سابقا

المبحث الأول

الجرائم المعلوماتية (مفهومها ، تطورها ، آثارها)

المطلب الأول : المقصود بالجرائم المعلوماتية
المطلب الثاني : أشكال الجرائم المعلوماتية
المطلب الثالث : صعوبة إثبات الجرائم المعلوماتية

المبحث الثاني

الأحكام والضوابط الواردة بخصوص الجرائم المعلوماتية في

النظام السعودي والأنظمة المقارنة

المطلب الأول : طبيعة الجرائم المعلوماتية
المطلب الثاني : مدى موافقة الأنظمة السعودية للصعوبات التي تعترض إثبات الجرائم المعلوماتية

الخاتمة

- النتائج
- التوصيات

قائمة المصادر والمراجع

المبحث الأول

الجرائم المعلوماتية (مفهومها ، تطورها ، آثارها)

يقسم هذا المبحث إلى ثلاثة مطالب :

المطلب الأول : المقصود بالجرائم المعلوماتية

المطلب الثاني : أشكال الجرائم المعلوماتية

المطلب الثالث : صعوبة إثبات الجرائم المعلوماتية

المطلب الأول

المقصود بالجرائم المعلوماتية

هناك عدة مسميات تدل على الجرائم المعلوماتية منها الجرائم الالكترونية ،جرائم التقنية العالية،جرائم الكمبيوتر والإنترنت ،والجرائم النظيفة وغيرها.(عبد المجيد ، 246) و تعرف بأنّها "كل نشاط عمدي يقصده الفاعل باستخدام تقنية المعلومات أو تكون تلك التقنية محلاً لهذا السلوك ،وذلك لأجل أحداث ما يجرمه القانون ويعاقب عليه. ".(الدلالعة ، 2010 ،9) وتعرف أيضاً بـ " هي الجريمة ذات الطابع المادي تتمثل في كل فعل أو سلوك غير مشروع مرتبط بأية وجهة بالحاسبات ،يتسبب في تكبد أو إمكانية تكبد المجني عليه خسارة ،وحصول أو أمكانية حصول مرتكبه على أي مكسب".(حسين، 2011 ،2)ويقصد بها كذلك " كل نشاط إجرامي يؤدى فيه نظام الكمبيوتر دوراً لإتمامه على أن يكون هذا الدور مؤثرا في ارتكاب الجريمة المعلوماتية على أن يراعى في كل الأحوال التطور السريع والمتلاحق لتكنولوجيا المعلومات والاتصالات ".(بكار،2010 ،184)

أما نظام مكافحة جرائم المعلوماتية السعودي لعام 1428هـ وفي المادة الأولى الفقرة (8)نجده قد عرف الجريمة المعلوماتية بأنَّها " أي فعل يرتكب متضمناً استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام" ،ثم أتى فيما بعد في مواده اللاحقة بتفصيل هذه الجرائم وتحديد لمرتكبيها بخلاف القانون رقم 5لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات في الإمارات العربية المتحدة " وهو قانون اتحادي" نجده لم يحدد تعريف للجريمة الإلكترونية ، وإنما سار على نهج النظام السعودي بأن فصل مواده اللاحقة الأفعال التي تندرج تحت الجرائم المعلوماتية محدداً في ذات الوقت كنتيجة طبيعية العقوبات التي توقع على من يخالفها ، وهو ما انسحب على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات[1].

١-صدرت بموجب القرار مجلس الوزراء رقم (162)وتاريخ 1433/5/24هـ.وبموافقة المقام السامي بالمرسوم رقم م- 35 وتاريخ 1433/5/25،وبتعميم وزير العدل رقم 13-ت-4601 وتاريخ 1433/6/8هـ

وهو ما سار عليه قانون الإمارات العربية الاسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها[1].

رأي الباحث :

ويرى الباحث أن النظام السعودي كان أفضل من غيره من الأنظمة بأنَّه أورد تعريفاً جامعاً لكل ما اتفق حوله كتاب القانون حول ما يعد جريمة معلوماتية ،ومن ثم لم يخالف نهج الأنظمة المقارنة الأخرى بكونه أورد تفصيلات هذا التعريف مفرداً في ذات الوقت العقوبات لكل قسم من أقسام هذه الجرائم حسب درجة خطورتها وآثارها على المجتمع السعودي.

وتبدو ايجابية النظام السعودي في إيراده لتعريف الجريمة المعلوماتية في استدراك ما لم يقع تحت حصر في مواده اللاحقة مستقبلاً ،ولعل هذا مرده إلى حداثة هذا النوع من الجرائم وما يصاحبها من تطور في كيفية ارتكابها ،الأمر الذي قد يصاحبه تباطؤ تشريعي لمواكبة هذا التغير ، وهو ما يمكن تداركه بنص التعريف الوارد في النظام.

١-وهو قانون عربي استرشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها تقدم به وزير العدل في دولة الإمارات العربية المتحدة بتاريخ 2001/12/19 إلى مجلس الوزراء العرب وتم اعتماده في مجلس وزراء العدل العرب في دورته التاسعة عشرة بالقرار رقم 495-د19-2003/10/8 ومجلس وزراء الداخلية العرب في دورته الحادية والعشرين بالقرار رقم 417-د2004/21— جدير بالذكر أن قانون جرائم أنظمة المعلومات لسنة 2010 الأردني سار على ذات النهج.

المطلب الثاني
أشكال الجرائم المعلوماتية

اعتمد كتاب القانون في تقسيمهم للجرائم المعلوماتية إلى أشكال مختلفة على عدة معايير منها الهدف من ارتكاب الجريمة والقدرات والمهارات التي يمتلكها الجاني .ولا يمكن أن نحدد تقسيمات على سبيل الحصر يمكن من خلالها أن نقول هذه الأقسام التي تندرج تحت عنوان الجرائم المعلوماتية، لأن هذه الجرائم في تطور مستمر تبعا لأسباب كثيرة أهمها تطور وسائل الاتصالات والمعلومات. [1](فاهد، 46،1432)لكن مع ذلك يمكن أن تقسم إلى أربع أشكال رئيسية على نحو ما يلي:

الشكل الأول :الجرائم العامة ومثالها إغفال الواجب والتقصير والإهمال والتآمر والتواطؤ.

الشكل الثاني: الجرائم الاقتصادية كالنصب والاحتيال والتهديد والتزييف والتزوير.(داود، 1420 ،38).

الشكل الثالث: جرائم الاعتداء على الأشخاص كالسب والقذف ،والاعتداء على حرمة الحياة الخاصة ،وجرائم الاستغلال الجنسي.

الشكل الرابع:الجرائم الواقعة على الأموال كالسرقة والتحويل غير المشروع وإتلاف برامج ومعلومات الحاسب الآلي. (العبيدي76،1428) ويعد البعض أن هذا التنوع في الأشكال مرجعه إلى الأساليب المتنوعة في ارتكاب مثل هذا النوع من الجرائم إذ إنَّ بعضها يقوم على أساليب فنية كالتجسس ونشر الفيروسات ،في حين يرى البعض أن هناك أنواع أخرى تعتمد بشكل أساسي على نقاط الضعف البشرية أو الاستخفاف بالعقول

1- بعضهم أضاف الجرائم السياسية انظر في ذلك:أ.عبدالرفيع ارويحن،مكافحة الجرائم الالكترونية قراءة في مؤتمر أبو ظبي بدول مجلس التعاون الخليجي ،قانون وأعمال،عدد 3 يونيو، 2007،ص62 ويرى الباحث أن نظام مكافحة الجرائم المعلوماتية لسنة 1428هـ قد أكد على ذات التقسيمات المذكورة في المتن من خلال الأهداف التالية أوردها في المادة الثانية منه وهى : 1/المساعدة على تحقيق الأمن المعلوماتي 2/حفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية والشبكات المعلوماتية 3/حماية المصلحة العامة ،والأخلاق /والآداب العامة. 4/حماية الاقتصاد الوطني

وذلك من خلال عرض معلومات ترويجية على الانترنت مفادها إمكانية الحصول على أرباح طائلة وبناء على ذلك يحصل الجاني على معلومات خاصة بالضحية كرقم الحساب البنكي.(ندوة الجرائم المعلوماتية وقضاياها المستجدة في المملكة العربية السعودية ،1429، 277).

وبالرجوع إلى نظام مكافحة جرائم المعلوماتية الصادر في العام 1428هـ[1]، نجده قد غطى جميع الأشكال والصور السابقة بتفريد عقابي يتناسب مع جسامة الفعل المرتكب والأثر المترتب عليه وهى في اعتقاد الباحث عقوبات مناسبة كافية للردع وتقلل من فرص ارتكاب الجرائم المعلوماتية.

١-يمكن الرجوع للمواد(6،5،4،3/7) من النظام المشار إليه وهى تقابل المواد (2___39) من القانون رقم 5 لسنة 2012 الإماراتي والخاص بمكافحة جرائم تقنية المعلومات والمواد (3_11) من قانون جرائم أنظمة المعلومات لسنة 2010 الأردني.

المطلب الثالث
صعوبة إثبات الجرائم المعلوماتية

تعدد أشكال الجرائم المعلوماتية بالإضافة إلى استخدام وسائل التقنية الحديثة كعنصر مهم لإتمام الفعل الإجرامي كل ذلك ألقى بظلاله على صعوبة إثبات الجرائم المعلوماتية وهو ما تلاحظ في الآتي:

أولاً:كونها ،لا تخلف ورائها أي أشياء مادية تعين في الوصول إلى مرتكب الجريمة بسهولة ومثاله انتفاء شهادة الشهود والمستندات الورقية ....الخ.(حسين،2011 ،3).

ثانياً:صعوبة تحريز المعلومات الخاصة بالجريمة (المشهد الرقمي،الدليل الرقمي)المرتكبة والتي تكون في غالب الأحوال الكترونيا ،الأمر الذي يتطلب بالضرورة مختصين يتولون التعامل معها،لأنَّه في بعض الأحوال إذا تم العثور على المعلومات المطلوبة وهذا مرجعه أما لطبيعة المواد مسرح الجريمة أو عدم التدريب الكافي،أو المعرفة التامة بأصول الأجهزة والبيانات الالكترونية لدى من يقوم بالضبط قد يكون سبباً في ضياع المعلومات المطلوبة والتي تدل بشكل كبير على الجاني.(بكار ،184)

ثالثاً:الاختلاف الزمني بين الدول يساعد المجرم في ارتكاب جريمته ويعقد في ذات الوقت من إجراءات التحري والتحقيق والتعاون حول تحديد هوية المجرم والقانون الذي سيطبق هذا في حالة ما إذا كان مكان ارتكاب الجريمة في دولة والأضرار المترتبة عليها لحقت بالمجني عليه في دولة أخرى ومثاله إطلاق الفيروسات المدمرة لمواقع شركات تجارية.(سياب ،13)

رابعاً:أن يعمد الجاني إلى عدم إعطاء شخصيته الحقيقية ،كأن ينتحل شخصية غيره ، أو يعطى عن نفسه معلومات مزيفة حتى يصعب من إمكانية الوصول إليه.(درف،18 2006)

خامساً:عدم إفصاح بعض الجهات (الضحية)كالمؤسسات المالية والشركات التجارية والبنوك من أنها قد تعرضت لهذا النوع من الجرائم حفاظا على ثقتها الائتمانية لدى عملائها أو خوفاً من الأضرار التي قد

تلحق بمركزها المالي،أو رغبة منها في عدم انتشار مثل هذه الأعمال بدواعي التقليد مثلا. (الهيتي،215)

سادساً:إمكانية الجاني من إزالة كل ما استعان به في ارتكاب الجريمة في فترة زمنية وجيزة في لحظة الضبط ،ومن ثم يمكنه إنكار فعله متعللاً بسوء الشبكة أو لخطأ أو عيب يرجع للجهاز المستخدم.(عيشة ،116)

بناء على ما سبق لاحظنا تطور وتعقيد الجرائم المعلوماتية باختلاف صورها ،هذا فضلاً عن الصعوبات التي تعترض إثباتها ،الأمر الذي يدعونا أن نبحث في الأنظمة السعودية ذات الصلة بالجرائم المعلوماتية بالمقارنة مع الأنظمة القانونية الأخرى ومن ثم مدى كفايتها من عدمه في الحد أو التقليل من هذه الجرائم للتحقق من الفرضيتين اللتين اشرنا لهما سابقا.

المبحث الثاني

الأحكام والضوابط الواردة بخصوص الجرائم المعلوماتية في النظام السعودي والأنظمة المقارنة

يتضح للناظر من أول وهلة أنَّ الجرائم المعلوماتية تنفرد بخصائص مختلفة تجعلها تتميز عن غيرها من الجرائم ،لذلك كان لابد لنا من الوقوف على هذه الطبيعة القانونية حتى نتمكن من الإدراك الكامل للإجراءات القانونية التي تتبع بشأنها حتى نتحقق من فعالية الأنظمة المتبعة في هذا الشأن وينقسم هذا المبحث إلى مطلبين :

المطلب الأول : طبيعة الجرائم المعلوماتية

المطلب الثاني : مدى موافقة الأنظمة السعودية للصعوبات التي تعترض إثبات الجرائم المعلوماتية.

المطلب الأول
طبيعة الجرائم المعلوماتية

تتجلى الطبيعة القانونية للجريمة المعلوماتية والتي تميزها عما سواها من الجرائم العادية أو التقليدية في نقطتين هما: (غنام ، 11)

أولاً:اتصاف الانترنت بالعالمية ،بالقدر الذي يمكن جميع الناس من الدخول إليه،فضلاً عن انتشاره في جميع أقطار العالم (وهو ما يشكل الإطار العام الذي ترتكب الجريمة من خلاله في أغلب الأحوال).

ثانياً:في أحيان كثيرة توجد شبكات تجمع مجموعة كبيرة من الأجهزة من أجل خدمة غرض أو هدف معين كما هو الحال في الشركات التجارية والوحدات الإدارية الحكومية.

هذه الطبيعة والذاتية المختلفة للجرائم المعلوماتية تتطلب قانون خاص بها يراعى جوانبها المختلفة فيما يتعلق بالإجراءات المتبعة في جمع أدلتها ،ثم التحقيق فيها ،وأخيراً إجراءات المحاكمة.

وتفصيل ذلك أن جمع الأدلة يتطلب وجود أشخاص مدربين يمتلكون القدرة الفنية اللازمة التي تعينهم في جمع المعلومات في مسرح الجريمة ،والتي قد تضيع أو تختفي للأبد أو حتى قد لا تكون مرئية له رغم وجودها كونه غير ملم بهذه المسائل الفنية لكون طبيعة المستندات الالكترونية تختلف عن المستندات العادية الأخرى وحتى يمكن تجاوز العقبة الأولى والجوهرية في إجراءات جمع الاستدلالات ومن ثم يساعد في إمكانية إثبات الجريمة المعلوماتية كنتيجة طبيعية لذلك [1] .

أما فيما يلي مرحلة التحقيق فهي تتطلب الدخول إلى المواقع الالكترونية الخاصة أو التنصت إلى المكالمات الهاتفية أو اعتراض المراسلات الالكترونية أو حتى تتبعها في حالة تجاوزها حدود الدولة إلى دولة أخرى ،إذن لابد من قواعد خاصة بالجرائم المعلوماتية تراعى ما هو مكفول بموجب الدساتير والأنظمة والاتفاقيات الدولية المقررة لحرمة الحياة الخاصة أو سيادة الدول والقواعد المنظمة للتفتيش بتحديد الجهة المختصة ومبررات إصدار الإذن ....الخ لأغراض التحقيق

١-انظر بشأن ذلك العوامل التي تؤدى إلى صعوبة إثبات الجرائم المعلوماتية والتي أشير لها في المطلب الثالث من المبحث الأول.

والتحري.وأخيرا فيما يتعلق بالمحاكمة فانَّ هنالك ضوابط خاصة لتحديد المحكمة المختصة بنظر الدعوى الجنائية لاسيما وأن هناك تباين في الأنظمة القانونية بشأن تحديد المحكمة المختصة وهو ما سنتطرق في المطلب القادم.

المطلب الثاني
مدى موافقة الأنظمة السعودية للصعوبات التي تعترض إثبات الجرائم المعلوماتية

تقدير فاعلية الأنظمة السعودية في الحد من الجرائم المعلوماتية يقتضى الوقوف على المعالجات التي اتبعتها السلطة التنظيمية بخصوص التغلب على الصعوبات التي تعترض إثبات الجرائم المعلوماتية هذا من ناحية ،ومن ناحية أخرى مراعاة التميز الواضح الذي أشار إليه الفقه القانوني لاختلاف الجرائم المعلوماتية عما سواها من الجرائم الجنائية التقليدية الأخرى والتي عالجها النظام الجزائي هذا كله مع المقارنة ببعض الأنظمة القانونية.

أولاً:فيما يخص تنظيم مكافحة الجرائم المعلوماتية في المملكة العربية السعودية فهناك نظام خاص بالجرائم المعلوماتية بموجب المرسوم الملكي رقم (17) للعام 1428هـ لتصبح بذلك الدولة العربية الثالثة، (البقمي،1،2008)التي تصدر نظاما يعالج مثل هذه الجرائم [1]، بينما تعد الإمارات العربية المتحدة أول دول عربية تصدر نظاما خاصا

١-الجدير بالذكر أن المملكة العربية السعودية قد نظمت كثير من التشريعات المحققة للحماية المعلوماتية منها نظام الاتصالات الصادر بالمرسوم الملكي رقم (م/ 12) بتاريخ 1422/3/12هـ،هذا بالإضافة إلى قرار مجلس الوزراء رقم (20) بتاريخ 1426/1/16هـ لتحقيق نظام المطبوعات والنشر بالمرسوم الملكي رقم (م/32) بتاريخ 1421/9/3هـ والذي نص على حماية برامج الحاسب الآلي. ونظام حماية حقوق المؤلف بالمرسوم الملكي رقم (م/41) بتاريخ 1424/7/2هـ ليحل محل نظام حماية حقوق المؤلف الصادر بالمرسوم الملكي (م/ 11) بتاريخ 1410/5/19هـ. ونظام التعاملات الالكترونية الصادر بالمرسوم الملكي(م/ 18) لسنة 1428هـ.وتنظيم هيئة الاتصالات السعودية لسنة 1422هـ.علما بأنه تم تعديل مسمى هيئة التحقيق والإدعاء العام ليكون "النيابة العامة" بموجب الأمر الملكي رقم أ/ 240 في 1438/9/22هـ

بمكافحة جرائم المعلومات حيث أصدرت القانون الاتحادي رقم (2) لسنة 2006تحت مسمى (قانون مكافحة جرائم تقنية المعلومات)[1].

ثانيا:فيما يتعلق بالأنظمة السعودية من الصعوبات التي تعترض مسار إثبات الجرائم المعلوماتية وبالأخص فيما يتعلق بالإجراءات المتبعة في جمع الأدلة ،نجد أن نظام مكافحة الجرائم المعلوماتية لسنة 1428هـ في المادة الخامسة عشرة منه ينص على: "تتولى هيئة التحقيق والادعاء العام في الجرائم الواردة في هذا النظام "[2] والتي تمارس إجراءاتها في التحقيق فيما وصل إليها من مضبوطات ومتهمين مستعينة بدليل إجراءات ضبط الجرائم المعلوماتية [3]. حيث يحتوى على كثير من البيانات التي يتعين على من يتولى الضبط من رجال الضبط الجنائي وفقا للمادة (24) من نظام الإجراءات الجزائية لسنة 1435هـ أن يراعيها ومثاله الإجراءات الخاصة بتحريز الأجهزة في مسرح الجريمة " حواسيب ،هواتف محمولة وأجهزة كفية ووسائل التخزين المختلفة " من قبل المختصين ،هذا فضلا عن البيانات التي يتعين توفيرها عند الضبط ،والتي تعين من يتولى التحقيق فيما بعد.

في تقدير الباحث ما من شك أن من شأن ما تمت الإشارة إليه أن يدحض أو على أسوأ تقدير يقلل من الصعوبات التي تناولها كتاب القانون

١-لاحقا صدر القانون رقم (5)لسنة 2012 الخاص بمكافحة جرائم تقنية المعلومات.

٢-بالرجوع إلى نظام الإجراءات الجزائية لسنه 1435هـ نجده قد اشتمل على عدة مواد منها المادة (13) والتي تنص على :(تتولى هيئة التحقيق والادعاء العام طبقا لنظامها ولائحته) أما المادة(25) فتنص على يخضع رجال الضبط الجنائي فيما يتعلق بوظائفهم في الضبط الجنائي المقررة في هذا النظام لإشراف هيئة التحقيق والادعاء العام .....) غنى عن البيان أن المادة (26) من ذات النظام المشار إليه قد حددت الفئات المخولة بأعمال الضبط الجنائي.

٣-تعميم رقم 44663 بتاريخ 1433/6/29هـ الصادر من صاحب السمو الملكي مساعد وزير الداخلية للشؤون الأمنية والخاص بالإجراءات والنماذج المطلوب استكمالها في ضبط الجرائم المعلوماتية.

فيما يتعلق بالتعامل مع المعلومات الخاصة بالجريمة الالكترونية لكون من يتعامل معها تنقصه المعرفة والخبرة الفنية اللازمتين في تحريز الأدلة بمسرح الجريمة ،وفى ذات الوقت يغطى الفجوة الأخرى التي أشار إليها القانونيون بشأن التمايز بين الجرائم المعلوماتية وغيرها من الجرائم إذ أن مرحلة الضبط والتحقيق تحتاج لكادر مؤهل ومدرب وهو ما تحققه الدورات والنشرات الخاصة بذلك والتي تصدرها الجهات المختصة من وقت لأخر .

وهو ما يأتي في تقدير الباحث متوافقا مع جملة التدابير والإجراءات التي أشار إليها بعض المختصين وما خلصت إليه مجمل ورش العمل في كيفية تحريز الدليل الرقمي لعدم إفلات المجرم بجريمته.(درف ،315)

ثالثا:فيما يتعلق بالإجراءات النظامية المتبعة بشأن إجراءات التحقيق .وما يقلل من صعوبة إثبات الجرائم المعلوماتية نستطيع أن نقول وبكل اطمئنان أن الأنظمة في المملكة العربية السعودية قد قطعت شوطا كبيرا في هذا المجال. وللتدليل على ما سبق فعلى سبيل المثال أن النظام قد أوجب على مزودي الخدمات التعاون مع رجال الضبط القضائي وهو ما أشارت إليه المادة (14) من نظام مكافحة الجرائم المعلوماتية لسنة 1428هـبالنص على : "تتولى هيئة الاتصالات وتقنية المعلومات وفقا لاختصاصها تقديم الدعم والمساندة الفنية للجهات الأمنية خلال مراحل ضبط هذه الجرائم والتحقيق فيها وأثناء المحاكمة"[1] .

١-سبق وان ذكرنا أن هناك إجماع عالمي بالحفاظ على خصوصية الأفراد فيما يتعلق بالمكالمات الهاتفية والمراسلات....الخ وهو ما أكدت عليه المادة (9) من نظام الاتصالات السعودي لسنة 1422هـ التي تنص على:(سرية المكالمات الهاتفية والمعلومات التي يتم إرسالها واستقبالها عن طريق شبكة الاتصالات العامة مصونة ، ولا يجوز الاطلاع عليها أو الاستماع إليها أو تسجيلها إلا في الحالات التي تتبناها الأنظمة).وكذلك ما أشارت إليه المادة (56)من نظام الإجراءات الجزائية لسنة 1435هـ.

جدير بالذكر أن ما تمت الإشارة إليه هناك اتجاه يدعمه في قانون الإجراءات الفرنسي الذي ينص في المادة (1/60) المعدلة بالقانون رقم 2004/204 الصادر فئ 9 مارس 2004 على:

" لمأمور الضبط القضائي أن يطلب من كل شخص ،من كل مؤسسة من كل جهة خاصة أو عامة لديه مستندات تتعلق بالتحريات الجارية ، ويدخل فيها تلك الصادرة عن أنظمة الكمبيوتر أو أنظمة المعلومات الاسمية أن يسلمه هذه المستندات دون أن يكون لهؤلاء أن يتمسكوا بدون وجه حق بالالتزام بسر المهنة . "،(غنام ،117)كما أشارت لذلك الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في المادة الخامسة والعشرين منها بعنوان (أمر تسليم المعلومات) والتي نصت على:

"تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأوامر إلى: (2) أي مزود خدمة يقدم خدماته في إقليم الدولة الطرف لتسليم معلومات المشترك المتعلقة بتلك الخدمات في حوزة مزود الخدمة أو تحت سيطرته ".إما المادة(26/ب)من ذات الاتفاقية بعنوان "تفتيش المعلومات المخزنة" تنص على :

"(2)تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من التفتيش أو الوصول إلى تقنية معلومات معينة أو جزء منها بما يتوافق مع الفقرة (1-أ) إذا كان هناك اعتقاد بأن المعلومات المخزنة في تقنية معلومات أخرى أو جزء منها في إقليمها وكانت هذه المعلومات قابلة للوصول قانونا أو متوفرة في التقنية الأولى فيجوز توسيع نطاق التفتيش والوصول للتقنية الأخرى".

والمادة (28) بعنوان: "الجمع الفوري لمعلومات تتبع المستخدمين"في الفقرة (1/ب) والتي تنص على : "إلزام مزود الخدمة ضمن اختصاصه الفني بأن:

- يجمع أو يسجل بواسطة الوسائل الفنية على إقليم تلك الدولة الطرف .

- يتعاون ويساعد السلطات المختصة في جمع وتسجيل معلومات تتبع المستخدمين بشكل فوري مع الاتصالات المعنية في إقليمها أو التي تثبت بواسطة تقنية المعلومات."

حيث تتجلى الفائدة التي يقدمها مزود الخدمة للمحقق في نقاط عديدة نذكر منها على سبيل المثال أطراف المراسلات الالكترونية أما عن طريق البريد الالكتروني أو المحادثات شفوية أو مكتوبة ،وتاريخ إجراء المكالمة، والمواقع التي دخل عليها العملاء ومن ثم يمكن قراءاتها والتي بلا شك تفيد ميول واتجاهات المستخدم ومن ثم معرفة النواحي الإجرامية التي يسعى إليها .أو حتى الاطلاع على بيانات المكالمات الهاتفية لمعرفة عدد مرات الاتصال واليوم والساعة ومدة المكالمة ومن قام بمهاتفتهم جميعا ومن ثم تحديد من هم في دائرة الاشتباه.[1]

تجدر الإشارة انه لا يمكن الاطلاع على مضمون ومحتوى المحادثات الهاتفية وغيرها من وسائل الاتصال أو حتى مراقبتها إلا بأمر مسبب ولمدة محدودة ،كما بإمكان رئيس هيئة التحقيق والادعاء العام أن يأذن بمراقبة المحادثات الهاتفية وتسجيلها متى ما كان هناك فائدة في ظهور معلومات خاصة بجريمة ارتكبت ،على أن يكون هذا الأمر مسببا ومحدداً لمدة لا تزيد عن عشرة أيام قابلة للتجديد وفقا لمقتضيات التحقيق[2].

رابعا:لم يحدد نظام مكافحة الجرائم المعلوماتية لسنة 1428هـ المحكمة المختصة وتبعا لذلك فان الاختصاص القضائي بجرائم المعلوماتية في المملكة العربية السعودية ينعقد للمحاكم الجزائية وفقا لاختصاصها العام بولاية النظر في جميع الدعاوى ذات الصبغة الجزائية .

ولكن مع ذلك تظل الإشكالية الكبرى إذا كانت الجريمة المعلوماتية عابرة للحدود ،وهو ما لا يمكن حله في اعتقاد الباحث إلاَّ عبر الاتفاقيات الخاصة ومثاله الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، وبالنظر

١-ملاحظة لا يجوز القبض أو توقيف أي مشتبه في غير حالات التلبس إلا بأمر من السلطة المختصة ٍانظر في ذلك المادة (35) من نظام الإجراءات الجزائية لسنة 1435هـ.

٢-المادتان (56) ،(57) من نظام الإجراءات الجزائية لسنة 1435هـ .

إلى قانون مكافحة جرائم تقنية المعلومات لسنة 2012 الإماراتي نجده أيضا لم يحدد المحكمة المختصة بنظرها ،مما يعنى انطباق القواعد العامة المنصوص عليها في قانون الإجراءات الجزائية في مادته (142) والتي أشارت إلى أن تحديد الاختصاص يكمن بالمكان الذي وقعت فيه الجريمة[1] .

خلاصة القول يمكن أن نقول أن نظام مكافحة جرائم المعلوماتية لسنة 1428هـ إضافة إلى نظام الإجراءات الجزائية لسنة 1435هـ ونظام هيئة الاتصالات وتقنية المعلومات قد وضعوا قواعد قانونية تسهم بقدر كبير في الحد من انتشار وارتكاب الجرائم المعلوماتية.

١-وهى تقابل المادتان (130) التي تنص على : (يتحدد الاختصاص المكاني للمحاكم في مكان وقوع الجريمة ،أو المكان الذي يقيم فيه المتهم ،فان لم يكن له مكان إقامة معروف يتحدد الاختصاص في المكان الذي يقبض عليه) .والمادة (131) التي تنص على : (يعد مكانا للجريمة كل مكان وقع فيه فعل من أفعالها ،أو ترك فعل يتعين القيام به حصل بسبب تركه ضرر جسدي) من نظام الإجراءات الجزائية لسنة 1425هـ .

الخاتمة

وهى تشتمل على النتائج والتوصيات على النحو التالي:

أولاً:النتائج

1- وجود دليل إجرائي فني خاص بضبط الأدلة في الجرائم المعلوماتية يدحض فكرة صعوبة جمع الاستدلالات في الجرائم المعلوماتية.

2- عدم وجود نص في نظام مكافحة الجرائم المعلوماتية لسنة 1428هـ يعنى بتحديد المحكمة ذات الاختصاص القضائي ، لا يعيق إجراءات المحاكمة إذ يمكن الرجوع للقواعد العامة في نظام الإجراءات الجزائية لسنة 1435هـ.

3- المساندة الفنية التي تتولى تقديمها هيئة الاتصالات وتقنية المعلومات يزيل كثيرا من الصعوبات التي ترتبط بالتحقيق والضبط والمحاكمة فيما يخص الجرائم المعلوماتية في المملكة العربية السعودية.

4- اتصاف الجرائم المعلوماتية بأنها عابرة للحدود يمكن أن تعالجها وتحد من انتشارها اتفاقيات التعاون الخاصة بها والتي تصادق عليها المملكة العربية السعودية .

ثانيا:التوصيات

1- إدراج نص محدد في نظام مكافحة الجرائم المعلوماتية لسنة 1428هـ يبين الاختصاص القضائي أسوة بالجرائم الأخرى التقليدية.

2- تشديد العقوبات في بعض أنواع الجرائم المعلوماتية بما يتفق مع جسامة الأثر المترتب على ارتكابها .

3- المراجعة المستمرة لنصوص نظام مكافحة الجرائم المعلوماتية لمواكبة التطور المتزايد في وسائل التقنية الحديثة من ناحية ،والتطور المصاحب لها في وسائل ارتكابها مما يؤدى لظهور إشكال جديدة.

قائمة المصادر والمراجع

- ارويحن، عبدالرفيع ،يونيو، 2007، مكافحة الجرائم الالكترونية(قراءة في مؤتمر أبو ظبي)بدول مجلس التعاون الخليجي ،قانون وأعمال،عدد 3.
- البقمي،ناصر بن محمد ، عرض لكتاب مكافحة الجرائم المعلوماتية وتطبيقاتها في دول مجلس التعاون لدول الخليج العربية،مركز الإمارات للدراسات والبحوث الإستراتيجية،ط1،2008)بمجلة شؤون خليجية ،عدد58،2009.
- بكار، الحسن ،اكتوبر2010،الطبيعة القانونية للجريمة المعلوماتية،مجلة الملف،عدد17.

تعميم رقم 44663 بتاريخ 1433/6/29هـ الصادر من صاحب السمو الملكي مساعد وزير الداخلية للشؤون الأمنية والخاص بالإجراءات والنماذج المطلوب استكمالها في ضبط الجرائم المعلوماتية.

– - التقرير السنوي لهيئة الاتصالات وتقنية المعلومات في المملكة العربية السعودية للعام1434/1435هـ(2013).

- حسين، فريحة ،أكتوبر 2011، الجرائم الالكترونية والانترنت،مجلة المعلوماتية ، عدد36.
- داود ، حسن طاهر ،1420هـ ،2000م ،جرائم نظم المعلومات ،مركز الدراسات والبحوث بأكاديمية نايف العربية للعلوم الأمنية ، ط1،الرياض.
- درف، عبدالله ،متطلبات هيئة الادعاء في الجرائم الالكترونية ،مجلة العدل التي تصدرها وزارة العدل السودانية ،السنة 8،عدد318،2006.
- الدلالعة، سامر محمود ،التحديات التشريعية لتقنية المعلومات في مجال الأمن الجنائي دراسة مقارنة ،مجلة المنارة ،مجلد 16،عدد2010.
- الدليل الفني الإجرائي الخاص بضبط وتحريز الأدلة في الجرائم

المعلوماتية صدر بموجب القرار مجلس الوزراء رقم (162)وتاريخ

1433/5/24هـ.وبموافقة المقام السامي بالمرسوم رقم م- 35 وتاريخ 1433/5/25،وبتعميم وزير العدل رقم 13-ت-4601 وتاريخ 1433/6/8هـ.

- سياب ،حكيم ،السمات المميزة للجرائم المعلوماتية عن الجرائم التقليدية ،دراسات وأبحاث ،مجلة دولية علمية محكمة .
- صحيفة الاقتصادية العدد(7360) بتاريخ الخميس الموافق الأول من صفر 1435هـ، 5/ديسمبر /2013 .
- عبدالمجيد، محمد سعيد ،الأبعاد الاجتماعية والتشريعية للجريمة الالكترونية ، مجلة كلية الآداب ،جامعة الزقازيق.
- العبيدي ،أسامة بن غانم ،محرم 1428هـ- يناير2008 ،جرائم الحاسب الآلي والانترنت،مجلة الإدارة العامة،عدد1،مجلد48، .
- عيشة، خلدون ،الطبيعة الخاصة للجريمة الالكترونية وصورها ،مجلة دراسات وأبحاث ،مجلة دولية علمية محكمة .
- غنام ،غنام محمد ،ذاتية الإجراءات الجنائية في مجال جرائم تقنية المعلومات.
- فاهد ،عبدالله سعيد ، 1432هـ ، 2011،مكافحة الجرائم الالكترونية،ط1،الرياض.
- قانون جرائم أنظمة المعلومات لسنة2010 الأردني.
- القانون رقم (5)لسنة2012 الخاص بمكافحة جرائم تقنية المعلومات.
- القانون رقم 5 لسنة 2012 الإماراتي والخاص بمكافحة جرائم تقنية المعلومات.
- ندوة الجرائم المعلوماتية وقضاياها المستجدة في المملكة العربية السعودية ،مجلة العدل ،عدد38،ربيع الأخر 1429هـ .
- نظام الاتصالات السعودي لسنة1422هـ .
- نظام الإجراءات الجزائية لسنه1435هـ[1].

- نظام مكافحة الجرائم المعلوماتية لسنة 1428هـ.
- الهيتي، محمد حماد مرهج ،جرائم الحاسوب (ماهيتها ،موضوعها ،أهم صورها ،والصعوبات التي تواجهها)،دار المناهج للنشر والتوزيع.