

جمهورية مصر العربية

محكمة النقض

**المواجهة الجنائية للجرائم الإلكترونية
فى ضوء أحكام قانون مكافحة جرائم تقنية المعلومات**

ورقة عمل مقدمة

للمؤتمر التاسع لرؤساء المحاكم العليا فى الدول العربية

المركز العربى للبحوث القانونية والقضائية

" مجلس وزراء العدل العرب - جامعة الدول العربية "

الفترة من ١٧ - ١٩ ديسمبر ٢٠١٨

بيروت - لبنان

مقدمة

كشفت السنوات الأخيرة النقاب عن تكنولوجيا متطورة لم تكشفها عقود من الزمن، وإزاء التطورات السريعة فى هذه التكنولوجيا التى جاءت لخدمة الإنسان، إلا أن البعض لم يحسن استخدامها وألحق الضرر بأخيه الإنسان، لنجد أنفسنا أمام صنوف شتى من الجرائم الإلكترونية.

ونظراً لحدائثة الجرائم الإلكترونية وظهورها مع كل تقنية حديثة يتم اكتشافها، تجد إساءة فى الاستخدام، مما يستوجب على المشرع المصرى مواكبة التطور الحاصل فى هذا المجال، وذلك من خلال استحداث نصوص تشريعية لمكافحة الجرائم الناتجة عن هذه التقنيات، ووضع حد لها، إن لم يكن فى الإمكان القضاء عليها.

ونظراً لأن مرتكبى الجرائم الإلكترونية يتمتعون بذكاء حاد مما يسهل لهم ارتكاب تلك الجرائم أو صعوبة إثباتها، والإفلات من العقاب، فضلاً عن أن كثيراً من هذه الجرائم ترتكب فى إطار عابر للحدود الوطنية، فإن كل ذلك يستتبع أهمية وجود تعاون دولى لمواجهة هذا النوع من الجرائم.

١- ماهية الجريمة الإلكترونية:

خلا قانون مكافحة جرائم تقنية المعلومات المصرى - الصادر بالقانون رقم ١٧٥ لسنة ٢٠١٨ - من تعريف للجريمة الإلكترونية، كغيره من التشريعات المقارنة فى هذا الشأن.

ومع ذلك فقد عرفت بعض من هذه التشريعات الجريمة الإلكترونية، فعرفها نظام مكافحة جرائم المعلومات السعودى بأنها " أى فعل يرتكب متضمناً استخدام الحاسب الآلى أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام^(١) .

(١) المادة ١/١ من نظام جرائم المعلوماتية السعودى رقم ١٧ لسنة ١٤٢٨هـ.

وعرف القانون الأمريكى الجريمة الإلكترونية بأنها " الاستخدام الغير مصرح به لأنظمة الكمبيوتر المحمية أو ملفات البيانات أو الاستخدام المتعمد الضار لأجهزة الكمبيوتر أو ملفات البيانات"^(١).

وبمطالعة أحكام قانون مكافحة جرائم تقنية المعلومات، يمكن تعريف الجريمة الإلكترونية بأنها كل فعل أو امتناع ينشأ عن الاستخدام غير المشروع لتقنية المعلومات.

٢- خصائص الجريمة الإلكترونية:

للجريمة الإلكترونية مجموعة من الخصائص تتفرد بها عن الجرائم التقليدية، فهذه الجرائم تتطلب وجود جهاز إلكترونى ومعرفة كيفية استخدامه، كما أن هذه الجريمة لا حدود لها، فضلاً عن أنها جريمة صعبة الإثبات والاكتشاف.

فأغلب الجرائم الإلكترونية ترتكب عبر الإنترنت، حيث تقع تلك الجرائم، فيكون المجرم فى دولة والمجنى عليه فى دولة أخرى، وقد يكون الضرر أو النتيجة الإجرامية فى دولة ثالثة أو عدة دول، مثل اختراق المواقع والأجهزة وإتلافها وسرقة البيانات والمعلومات والأموال، كل ذلك جعل من مكافحة الجريمة الإلكترونية أمراً عسيراً، وذلك لتعدد الأماكن التى تتعلق بالجريمة، وتنازع قوانين الدول الواجبة التطبيق، واختلاف الإجراءات الجنائية من دولة إلى أخرى.

وأخيراً فالجريمة الإلكترونية لا تترك آثاراً خارجية مادية، فهى جرائم نظيفة أى لا تترك آثاراً مادية ملموسة، ولذلك كانت هذه الجرائم صعبة الاكتشاف والإثبات.

ومما يزيد من صعوبة اكتشاف وإثبات الجرائم الإلكترونية، البعد الجغرافى بين الجانى والمجنى عليه، واستخدام الجانى وسائل تقنية حديثة فى ارتكاب جريمته، كما أن هذه الجريمة ترتكب فى وقت سريع، ويتم محو آثارها فى وقت أسرع لا يتعدى الثوانى، فضلاً عن عدم وجود خبرة لدى القائمين على مكافحة هذه الجرائم من ناحية البحث والتحقيق.

(١) المادة الأولى من القانون الأمريكى رقم ١٢١٣ لسنة ١٩٨٦ بمواجهة جرائم الكمبيوتر، أشار إليه د/ رامى متولى

القاضى، مكافحة الجرائم المعلوماتية، ٢٠١١، ص ٢٣.

٣- خطة البحث:

سنعرض لموضوع المواجهة الجنائية للجرائم الإلكترونية - فى ضوء قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ - وذلك من خلال ثلاثة مباحث وخاتمة، على النحو التالى:

المبحث الأول: الأحكام الموضوعية لمكافحة الجرائم الإلكترونية.

المبحث الثانى: الأحكام الإجرائية لمكافحة الجرائم الإلكترونية.

المبحث الثالث: نطاق تطبيق قانون مكافحة جرائم تقنية المعلومات من حيث المكان.

الخاتمة: النتائج والتوصيات.

المبحث الأول

الأحكام الموضوعية لمكافحة الجرائم الإلكترونية

لم تعد القواعد العامة فى قانون العقوبات كافية لمواجهة التعاملات الإلكترونية، وما قد ينجم عنها من جرائم إلكترونية، ومن ثم بدت الحاجة إلى تشريعات لمواجهة تلك الجرائم.

ونظراً لحدائثة الجرائم الإلكترونية، وظهر هذا النوع من الجرائم مع كل تقنية حديثة من تقنيات المعلومات، فقد سعى المشرع المصرى لمواكبة هذا التطور الحاصل فى هذا المجال، وذلك من خلال استحداث نصوص وأحكام موضوعية لمكافحة ومواجهة الجرائم الإلكترونية.

وهدياً بما تقدم، فسوف نعرض للأحكام الموضوعية لمواجهة الجرائم الإلكترونية من خلال خمسة مطالب على النحو التالى:

المطلب الأول: الاعتداء على سلامة شبكات وأنظمة تقنيات المعلومات.

المطلب الثانى: الجرائم المرتكبة بواسطة أنظمة وتقنيات المعلومات.

المطلب الثالث: جرائم الاعتداء على حرمة الحياة الخاصة والمحتوى

المعلوماتى غير المشروع.

المطلب الرابع: الجرائم المرتكبة من مدير الموقع.

المطلب الخامس: جرائم مقدمى الخدمة.

المطلب الأول

الاعتداء على سلامة شبكات وأنظمة تقنيات المعلومات

أولاً: جريمة الانتفاع بدون حق بخدمات الاتصالات والمعلومات وتقنياتها.

يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر، وبغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز خمسين ألف جنيه، أو بإحدى هاتين العقوبتين، كل من انتفع بدون وجه حق عن طريق شبكة النظام المعلوماتي أو إحدى وسائل تقنية المعلومات بخدمة اتصالات أو خدمة من خدمات قنوات البث المسموع أو المرئي^(١).

ويقصد بالشبكة المعلوماتية، مجموعة من الأجهزة أو نظم المعلومات تكون مرتبطة معاً، ويمكنها تبادل المعلومات والاتصالات فيما بينها، ومنها الشبكات الخاصة والعامّة وشبكات المعلومات الدولية؛ والتطبيقات المستخدمة عليها^(٢).

والنظام المعلوماتي هو مجموعة برامج وأدوات معدة لغرض إدارة ومعالجة البيانات والمعلومات، أو تقديم خدمة معلوماتية.

وعرف المشرع تقنية المعلومات بأنها أي وسيلة أو مجموعة وسائل مترابطة أو غير مترابطة تستخدم لتخزين واسترجاع وترتيب وتنظيم ومعالجة وتطوير وتبادل المعلومات أو البيانات، ويشمل ذلك كل ما يرتبط بالوسيلة أو الوسائل المستخدمة سلكياً أو لاسلكياً^(٣).

(١) المادة ١١ من القانون رقم ١٧٥ لسنة ٢٠١٨ في شأن مكافحة جرائم تقنية المعلومات.

(٢) المادة الأولى من القانون رقم ١٧٥ لسنة ٢٠١٨ في شأن مكافحة جرائم تقنية المعلومات.

(٣) المادة الأولى من القانون رقم ١٧٥ لسنة ٢٠١٨ في شأن مكافحة جرائم تقنية المعلومات.

ثانياً: جريمة الدخول غير المشروع للمواقع أو الحسابات الخاصة أو النظام المعلوماتي.

يعاقب بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من دخل عمداً، أو دخل بخطأ غير عمدى وبقي بدون وجه حق، على موقع أو حساب خاص أو نظام معلوماتي محظور الدخول عليه. فإذا نتج عن ذلك، إتلاف أو محو أو تغيير أو نسخ أو إعادة نشر للبيانات أو المعلومات الموجودة على ذلك الموقع أو الحساب الخاص أو النظام المعلوماتي، تكون العقوبة الحبس مدة لا تقل عن سنتين، وغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مائتي ألف جنيه أو بإحدى هاتين العقوبتين^(١).

ثالثاً: جريمة تجاوز حدود الحق فى الدخول إلى موقع أو حساب خاص أو نظام معلوماتي.

جرم المشرع فعل أى شخص يقوم بالدخول إلى المواقع أو الحسابات الخاصة أو أى نظام معلوماتي، وذلك باستخدام الحق المخول له، ولكنه يتعدى حدود هذا الحق سواء من حيث الزمان أو مستوى الدخول.

حيث قررت المادة الخامسة عشرة من القانون بأنه " يعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن ثلاثين ألف جنيه ولا تجاوز خمسين ألف جنيه، أو بإحدى هاتين العقوبتين، كل من دخل إلى موقع أو حساب خاص أو نظام معلوماتي مستخدماً حقاً مخولاً له، فتعدى حدود هذا الحق من حيث الزمان أو مستوى الدخول."

رابعاً: جريمة الاعتراض غير المشروع.

يعاقب بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائتين وخمسين ألف جنيه، أو بإحدى هاتين العقوبتين، كل من اعترض بدون وجه

(١) المادة ١٤ من القانون رقم ١٧٥ لسنة ٢٠١٨ فى شأن مكافحة جرائم تقنية المعلومات.

حق أى معلومات أو بيانات أو كل ما هو متداول عن طريق شبكة معلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها^(١).

ويقصد بالاعتراض مشاهدة البيانات أو المعلومات أو الحصول عليها، بغرض التنصت أو التعطيل أو التخزين أو النسخ أو التسجيل أو تغيير المحتوى أو إساءة الاستخدام أو تعديل المسار أو إعادة التوجيه، وذلك لأسباب غير مشروعة وبدون وجه حق^(٢).

خامساً: جريمة الاعتداء على سلامة البيانات والمعلومات والنظم المعلوماتية.

تشمل هذه الجريمة، الإتيان العمومى أو التعطيل أو تعديل المسار، أو الإلغاء الكلى أو الجزئى المتعمد، وبدون وجه حق للبرامج أو البيانات المخزنة أو المعالجة أو المولدة أو المخلفة على أى نظام معلوماتى وما فى حكمه، وذلك أياً كانت الوسيلة المستخدمة فى الجريمة.

حيث قررت المادة السابعة عشرة من قانون مكافحة جرائم تقنية المعلومات بأنه " يعاقب بالحبس مدة لا تقل عن سنتين، وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من أتلف أو عطل أو عدل مسار أو ألغى كلياً أو جزئياً متعمداً وبدون وجه حق البرامج والبيانات أو المعلومات المخزنة، أو المعالجة، أو المولدة أو المخلفة على أى نظام معلوماتى وما فى حكمه، أياً كانت الوسيلة التي استخدمت في الجريمة ".

ويقصد بالبيانات والمعلومات الإلكترونية كل ما يمكن إنشاؤه أو تخزينه أو معالجته أو تخليقه أو نقله أو مشاركته أو نسخه، بواسطة تقنية المعلومات كالأرقام والأكواد والشفرات والحروف والرموز والإشارات والصور والأصوات، وما فى حكمها.

والبيانات والمعلومات الإلكترونية، قد تكون بيانات شخصية، أو بيانات حكومية.

(١) المادة ١٦ من القانون رقم ١٧٥ لسنة ٢٠١٨ فى شأن مكافحة جرائم تقنية المعلومات.

(٢) المادة الأولى من قانون مكافحة جرائم تقنية المعلومات.

ويقصد بالبيانات الشخصية أى بيانات متعلقة بشخص طبيعي محدد أو يمكن تحديده، بشكل مباشر أو غير مباشر عن طريق الربط بينها وبين بيانات أخرى.

والمقصود بالبيانات الحكومية، البيانات المتعلقة بالدولة أو إحدى سلطاتها، أو أجهزتها أو وحداتها، أو الهيئات العامة، أو الهيئات المستقلة أو الأجهزة الرقابية، وغيرها من الأشخاص الاعتبارية العامة وما في حكمها، والمتاحة على الشبكة المعلوماتية أو على أي نظام معلوماتي أو على حاسب أو ما في حكمها.

والمعالجة الإلكترونية هى أي عملية إلكترونية أو تقنية تتم كلياً أو جزئياً، لكتابة أو تجميع أو تسجيل أو حفظ أو تخزين أو دمج أو عرض أو إرسال أو استقبال أو تداول أو نشر أو محو أو تغيير أو تعديل أو استرجاع أو استبدال البيانات والمعلومات الإلكترونية، وذلك باستخدام أي وسيط من الوسائط أو الحاسبات أو الأجهزة الأخرى الإلكترونية أو المغناطيسية أو الضوئية أو ما يُستحدث من تقنيات أو وسائط أخرى^(١).

سادساً: جريمة الاعتداء على البريد الإلكتروني أو المواقع أو الحسابات الخاصة.

حرصاً من المشرع على حماية البريد الإلكتروني أو الموقع أو الحسابات الخاصة، فقد جرم المشرع كل أفعال الإتلاف أو التعطيل أو الإبطاء أو الاختراق للبريد الإلكتروني أو المواقع أو الحسابات الخاصة بأحد الناس.

وشدد المشرع العقوبة إذا وقعت الجريمة على بريد إلكتروني أو موقع أو حساب خاص بأحد الأشخاص الاعتبارية الخاصة.

حيث قررت المادة الثامنة عشرة من قانون مكافحة جرائم تقنية المعلومات بأنه " يعاقب بالحبس مدة لا تقل عن شهر، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين كل من أتلف أو عطل أو أبطأ أو اخترق بريداً إلكترونياً أو موقعاً أو حساباً خاصاً بأحد الناس. فإذا وقعت الجريمة على بريد إلكتروني

(١) المادة الأولى من قانون مكافحة جرائم تقنية المعلومات.

أو موقع أو حساب خاص بأحد الأشخاص الاعتبارية الخاصة، تكون العقوبة الحبس مدة لا تقل عن ستة أشهر وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين.

ويقصد بالحساب الخاص، مجموعة من المعلومات الخاصة بشخص طبيعي أو اعتباري، تخول له دون غيره الحق في الدخول على الخدمات المتاحة أو استخدامها من خلال موقع أو نظام معلوماتي.

والبريد الإلكتروني هو وسيلة لتبادل رسائل إلكترونية على عنوان محدد، بين أكثر من شخص طبيعي و إعتباري، عبر شبكة معلوماتية، أو غيرها من وسائل الربط الإلكترونية، من خلال أجهزة الحاسب الآلى وما في حكمها.

سابعاً: جريمة الاعتداء على تصميم موقع.

حماية للموقع، فقد جرم المشرع إتلاف أو تعطيل أو إبطاء أو تشويه أو إخفاء أو تغيير تصاميم موقع خاص بشركة أو مؤسسة أو منشأة أو شخص طبيعي، وذلك بدون وجه حق.

فيعاقب بالحبس مدة لا تقل عن ثلاثة أشهر، وبغرامة لا تقل عن عشرين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من أتلف أو عطل أو أبطأ أو شوه أو أخفي، أو غير تصاميم موقع خاص بشركة أو مؤسسة أو منشأة أو شخص طبيعي بغير وجه حق^(١).

والموقع هو نطاق أو مكان افتراضي له عنوان محدد على شبكة معلوماتية^(٢).

(١) المادة التاسعة عشرة من قانون مكافحة جرائم تقنية المعلومات.

(٢) المادة الأولى من قانون مكافحة جرائم تقنية المعلومات.

ثامناً: جرائم الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة.

يعاقب بالحبس مدة لا تقل عن سنتين، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين، كل من دخل عمداً، أو دخل بخطأ غير عمدى وبقي بدون وجه حق، أو تجاوز حدود الحق المخول له من حيث الزمان أو مستوى الدخول أو اخترق موقعاً أو بريداً إلكترونياً أو حساباً خاصاً أو نظاماً معلوماتياً يدار بمعرفة أو لحساب الدولة أو أحد الأشخاص الاعتبارية العامة، أو مملوكاً لها، أو يخصصها.

فإذا كان الدخول بقصد الاعتراض أو الحصول بدون وجه حق على بيانات أو معلومات حكومية، تكون العقوبة السجن، والغرامة التي لا تقل عن مائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه.

وفى جميع الأحوال، إذا ترتب على أى من الأفعال السابقة إتلاف تلك البيانات أو المعلومات أو ذلك الموقع أو الحساب الخاص أو النظام المعلوماتى أو البريد الإلكتروني، أو تدميرها أو تشويهها أو تغييرها أو تغيير تصاميمها أو نسخها أو تسجيلها أو تعديل مسارها أو إعادة نشرها، أو إلغاؤها كلياً أو جزئياً، بأى وسيلة كانت، تكون العقوبة السجن، والغرامة التي لا تقل عن مليون جنيه ولا تجاوز خمسة ملايين جنيه.

وباستقراء نص المادة العشرين - سألقة البيان - يتضح تعدد جرائم الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة على النحو التالى:

١- جريمة الدخول العمدى لموقع أو بريد إلكترونى أو حساب خاص أو نظام معلوماتى يُدار بمعرفة أو لحساب الدولة أو أحد الأشخاص الاعتبارية العامة، أو مملوكاتها أو يخصصها.

٢- جريمة الدخول خطأ والبقاء بدون وجه حق لموقع أو بريد إلكترونى أو حساب خاص أو نظام معلوماتى، المشار إليهم بالبند (١).

٣- جريمة تجاوز حدود الحق المخول من حيث الزمان أو مستوى الدخول لموقع أو بريد إلكتروني أو حساب خاص أو نظام معلوماتي، المشار إليهم بالبند (١).

٤- جريمة اختراق موقع أو بريد إلكتروني أو حساب خاص أو نظام معلوماتي المشار إليه بالبند (١) ^(١).

٥- جريمة الدخول لموقع أو بريد إلكتروني أو حساب خاص أو نظام معلوماتي - المشار إليهم بالبند (١) - بقصد الاعتراض أو الحصول بدون وجه حق على بيانات أو معلومات حكومية ^(٢).

٦- جريمة ارتكاب أى من الأفعال المشار إليهم فى البنود من (١) إلى (٥) وترتب عليها إتلاف البيانات أو المعلومات أو الموقع أو الحساب الخاص أو النظام المعلوماتي أو البريد الإلكتروني، أو تدميرها أو تشويهها أو تغييرها أو تغيير تصاميمها أو نسخها أو تسجيلها أو تعديل مسارها أو إعادة نشرها، أو إلغاؤها كلياً أو جزئياً بأى وسيلة كانت.

وتكون العقوبة السجن، والغرامة التى لا تقل عن مليون جنيه ولا تجاوز خمسة ملايين جنيه.

تاسعاً: جريمة الاعتداء على سلامة الشبكة المعلوماتية ^(٣).

١- التسبب العمدى فى إيقاف الشبكة المعلوماتية عن العمل أو تعطيلها أو الحد من كفاءة عملها.

يعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من تسبب متعمداً في إيقاف شبكة معلوماتية عن العمل أو تعطيلها أو الحد من كفاءة عملها أو

(١) العقوبة فى البنود (١) إلى (٤) هى الحبس مدة لا تقل عن سنتين، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائتى ألف جنيه، أو بإحدى هاتين العقوبتين.

(٢) تكون العقوبة السجن، والغرامة التى لا تقل عن مائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه.

(٣) المادة ٢١ من قانون مكافحة جرائم تقنية المعلومات.

التشويش عليها أو إعاقتها أو اعتراض عملها أو أجرى بدون وجه حق معالجة إلكترونية للبيانات الخاصة بها.

٢- **التسبب خطأً فى إيقاف الشبكة المعلوماتية عن العمل أو تعطيلها أو الحد من كفاءة عملها.**

يعاقب كل من تسبب بخطئه فى إيقاف الشبكة المعلوماتية عن العمل أو تعطيلها أو الحد من كفاءة عملها، بالحبس مدة لا تقل عن ثلاثة أشهر، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائتى ألف جنيه، أو بإحدى هاتين العقوبتين.

٣- **تشديد العقوبة حال وقوع الجريمة على شبكة معلوماتية تخص الدولة أو أحد الأشخاص الاعتبارية العامة أو مملوكة لها أو مدارة بمعرفتها.**

تكون العقوبة السجن المشدد، وغرامة لا تقل عن خمسمائة ألف جنيه ولا تجاوز مليون جنيه، إذا وقعت الجريمة على شبكة معلوماتية تخص الدولة أو أحد الأشخاص الاعتبارية العامة أو تمتلكها أو تُدار بمعرفتها.

عاشراً: **جريمة حيازة أو إحراز أو جلب أو بيع أو إنتاج أو صنع أو استيراد أو تداول أجهزة بدون تصريح من الجهاز القومى لتنظيم الاتصالات، أو بدون مسوغ من الواقع أو القانون.**

يعاقب بالحبس مدة لا تقل عن سنتين، وبغرامة لا تقل عن ثلاثمائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من حاز أو أحرز أو جلب أو باع أو أتاح أو صنع أو أنتج أو استورد أو صدر أو تداول بأى صورة من صور التداول، أى أجهزة أو معدات أو أدوات أو برامج مصممة أو مطورة أو محورة أو أكواد مرور أو شفرات أو رموز أو أى بيانات مماثلة، بدون تصريح من الجهاز أو مسوغ من الواقع أو القانون، وثبت أن ذلك السلوك كان بغرض استخدام أى منها فى ارتكاب أو تسهيل

ارتكاب أى جريمة من الجرائم المنصوص عليها فى هذا القانون، أو إخفاء آثارها أو أدلتها أو ثبت ذلك الاستخدام أو التسهيل أو الإخفاء^(١).

ويشترط لتحقيق هذه الجريمة - فضلاً عن الركن المادى والقصد الجنائى العام - توافر قصد جنائى خاص يتمثل فى ارتكاب إحدى صور السلوك الإجرامى بغرض استخدام أى منها فى ارتكاب أو تسهيل ارتكاب أى جريمة من الجرائم المنصوص عليها فى قانون مكافحة جرائم تقنية المعلومات، أو إخفاء آثارها أو أدلتها، أو ثبوت ذلك الاستخدام أو التسهيل أو الإخفاء.

المطلب الثانى

الجرائم المرتكبة بواسطة أنظمة وتقنيات المعلومات

أولاً: جرائم الاحتيال والاعتداء على بطاقات البنوك وأدوات الدفع الإلكترونية.

عرض المشرع لجرائم الاحتيال والاعتداء على بطاقات البنوك والخدمات وأدوات الدفع الإلكترونية فى المادة ٢٣ من قانون مكافحة جرائم تقنية المعلومات، حيث قررت بأنه " يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر، وبغرامة لا تقل عن ثلاثين ألف جنيه، ولا تجاوز خمسين ألف جنيه، أو بإحدى هاتين العقوبتين، كل من استخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، فى الوصول بدون وجه حق إلى أرقام أو بيانات بطاقات البنوك والخدمات أو غيرها من أدوات الدفع الإلكترونية.

فإن قصد من ذلك استخدامها فى الحصول على أموال الغير أو ما تنتجه من خدمات يعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين.

(١) المادة ٢٢ من قانون مكافحة جرائم تقنية المعلومات.

وتكون العقوبة الحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مائتي ألف جنيه، أو إحدى هاتين العقوبتين، إذا توصل من ذلك إلي الاستيلاء لنفسه أو لغيره على تلك الخدمات أو مال الغير.

وبمطالعة المادة سالفه البيان، تجد أنها قد حوت ثلاثة أنواع من الجرائم، وذلك على النحو التالي:

الجريمة الأولى: استخدام الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات في الوصول - بدون وجه حق - إلى أرقام أو بيانات بطاقات البنوك والخدمات أو غيرها من أدوات الدفع الإلكترونية^(١).

فتتحقق هذه الجريمة بمجرد استخدام الشبكة المعلوماتية أو إحدى وسائل المعلومات في الوصول إلى بيانات أو بطاقات البنوك أو غيرها من أدوات الدفع الإلكترونية.

الجريمة الثانية: استخدام الوسائل المشار إليها في الجريمة الأولى بقصد الحصول على أموال الغير أو ما يتيح من خدمات^(٢).

الجريمة الثالثة: جريمة استخدام الوسائل المشار إليها في الجريمة الأولى والتوصل فعلاً إلى استيلاء الجاني لنفسه أو لغيره على تلك الخدمات أو مال الغير^(٣).

ثانياً: جرائم اصطناع موقع أو حساب خاص أو بريد إلكتروني ونسبته زوراً إلى شخص طبيعي أو اعتباري.

(١) العقوبة الحبس مدة لا تقل عن ثلاثة أشهر، وبغرامة لا تقل عن ثلاثين ألف جنيه ولا تجاوز خمسين ألف جنيه أو بإحدى هاتين العقوبتين.

(٢) تكون العقوبة الحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه أو بإحدى هاتين العقوبتين.

(٣) تكون العقوبة الحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين.

حرص المشرع على تجريم أفعال اصطناع بريد إلكتروني أو موقع أو حساب خاص ونسبته زوراً إلى شخص طبيعي أو اعتباري.

حيث قررت المادة ٢٤ من قانون مكافحة جرائم تقنية المعلومات بأنه " يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر، وبغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز ثلاثين ألف جنيه أو بإحدى هاتين العقوبتين، كل من اصطنع بريداً إلكترونياً أو موقعاً أو حساباً خاصاً ونسبه زوراً إلى شخص طبيعي أو اعتباري.

فإذا استخدم الجاني البريد أو الموقع أو الحساب الخاص المصطنع في أمر يسيء إلى ما نسب إليه، تكون العقوبة الحبس الذي لا تقل مدته عن سنة، والغرامة التي لا تقل عن خمسين ألف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى العقوبتين.

وإذا وقعت الجريمة على أحد الأشخاص الاعتبارية العامة، تكون العقوبة السجن، والغرامة التي لا تقل عن مائة ألف جنيه، ولا تزيد على ثلاثمائة ألف جنيه.

وتتحقق هذه الجريمة بمجرد اصطناع بريد إلكتروني أو موقع أو حساب خاص ونسبته زوراً إلى شخص طبيعي أو اعتباري.

وشدد المشرع العقوبة إذا وقعت تلك الجريمة في حالتين:

الحالة الأولى:

استخدام الجاني البريد أو الموقع أو الحساب الخاص المصطنع في أمر يسيء إلى ما نسب إليه، وتكون العقوبة الحبس مدة لا تقل عن سنة، والغرامة التي لا تقل عن خمسين ألف جنيه، أو بإحدى هاتين العقوبتين.

الحالة الثانية:

وقوع الجريمة على أحد الأشخاص الاعتبارية العامة^(١) وتنتقل الجريمة من جنحة إلى جنائية عقوبتها السجن، والغرامة التي لا تقل عن مائة ألف جنيه، ولا تزيد على ثلاثمائة ألف جنيه.

(١) حدد المشرع الأشخاص الاعتبارية في المادة ٥٢ من القانون المدني، حيث قررت بأن " الأشخاص الاعتبارية هي: ١- الدولة وكذلك المديرية والمدن والقرى والشروط التي يحددها القانون والإدارات والمصالح وغيرها من المنشآت العامة التي يمنحها القانون شخصية اعتبارية. ٢- الهيئات والطوائف الدينية التي تعترف لها الدولة بشخصية اعتبارية. ٣- الأوقاف. ٤- الشركات التجارية والمدنية. ٥- الجمعيات والمؤسسات المنشأة وفقاً لأحكام القانون. ٦- كل مجموعة من الأشخاص أو الأموال تثبت لها الشخصية الاعتبارية بمقتضى نص القانون.

المطلب الثالث

جرائم الاعتداء على حرمة الحياة الخاصة والمحتوى المعلوماتى غير المشروع

أولاً: جرائم الاعتداء على حرمة الحياة الخاصة.

حرص المشرع على تأكيد حماية حرمة الحياة الخاصة للمواطنين من الاعتداء عليها - والتي نُص عليها في الدستور المصرى^(١) - وذلك فى المادة ٢٥ من قانون مكافحة جرائم تقنية المعلومات، والتي قررت بأنه " يعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من اعتدى على أى من المبادئ أو القيم الأسرية فى المجتمع المصرى، أو انتهك حرمة الحياة الخاصة أو أرسل بكثافة العديد من الرسائل الإلكترونية لشخص معين دون موافقته، أو منح بيانات شخصية إلى نظام أو موقع إلكترونى لترويج السلع أو الخدمات دون موافقته أو نشر عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات، معلومات أو أخباراً أو صوراً وما فى حكمها، تنتهك خصوصية أى شخص دون رضاه، سواء كانت المعلومات المنشورة صحيحة أو غير صحيحة."

وتتعدد صور الجرائم المشار إليها فى المادة ٢٥ سالفه البيان، كما يلى:

- ١- جريمة الاعتداء على أى من المبادئ أو القيم الأسرية فى المجتمع المصرى.
- ٢- جريمة انتهاك حرمة الحياة الخاصة.
- ٣- جريمة إرسال العديد من الرسائل الإلكترونية لشخص معين دون موافقته.

(١) تقرر المادة ٩٩ من الدستور المصرى بأنه " كل اعتداء على الحرية الشخصية أو حرمة الحياة الخاصة للمواطنين، وغيرها من الحقوق والحريات العامة التى يكفلها الدستور والقانون، جريمة لا تسقط الدعوى الجنائية ولا المدنية الناشئة عنها بالتقادم، وللمضرور إقامة الدعوى الجنائية بالطريق المباشر. وتكفل الدولة تعويضاً عادلاً لمن وقع عليه الاعتداء، ولللمجلس القومى لحقوق الإنسان إبلاغ النيابة العامة عن أى انتهاك لهذه الحقوق، وله أن يتدخل فى الدعوى المدنية منضماً إلى المضرور بناء على طلبه، وذلك كله على الوجه المبين بالقانون."

٤- جريمة منح بيانات شخصية إلى نظام أو موقع إلكتروني لترويج السلع أو الخدمات دون موافقته.

٥- جريمة نشر معلومات أو أخبار أو صور - وما فى حكمها - تنتهك خصوصية أى شخص دون رضاه، وذلك عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات.

وتقع هذه الجريمة الأخيرة، بمجرد نشر المعلومات أو الأخبار أو الصور - وما فى حكمها - وسواء أكانت المعلومات المنشورة صحيحة أو غير صحيحة.

ثانياً: جريمة استعمال برنامج معلوماتي أو تقنية معلوماتية فى معالجة معطيات شخصية للغير لربطها بمحتوى مناف للآداب العامة.

يعاقب بالحبس مدة لا تقل عن سنتين ولا تجاوز خمس سنوات، وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز ثلاثمائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من تعدد استعمال برنامج معلوماتي أو تقنية معلوماتية فى معالجة معطيات شخصية للغير لربطها بمحتوى مناف للآداب العامة، أو لإظهارها بطريقة من شأنها المساس باعتباره أو شرفه^(١).

ويقصد بالبرنامج المعلوماتي، مجموعة الأوامر والتعليمات المعبر عنها بأية لغة أو رمز أو إشارة، والتي تتخذ أي شكل من الأشكال، ويمكن استخدامها بطريق مباشر أو غير مباشر فى حاسب آلي لأداء وظيفة أو تحقيق نتيجة، سواء كانت هذه الأوامر والتعليمات فى شكلها الأصلي أو فى أي شكل آخر تظهر فيه من خلال حاسب آلي، أو نظام معلوماتي.

وعرف المشرع تقنية المعلومات بأنها " أى وسيلة أو مجموعة وسائل مترابطة أو غير مترابطة تُستخدم لتخزين واسترجاع وترتيب وتنظيم ومعالجة وتطوير وتبادل

(١) المادة ٢٦ من قانون مكافحة جرائم تقنية المعلومات.

المعلومات أو البيانات، ويشمل ذلك كل ما يرتبط بالوسيلة أو الوسائل المستخدمة سلكياً أو لاسلكياً".

والمقصود بالمعالجة الإلكترونية، أى عملية إلكترونية أو تقنية تتم كلياً أو جزئياً، لكتابة أو تجميع أو تسجيل أو حفظ أو تخزين أو دمج أو عرض أو إرسال أو استقبال أو تداول أو نشر أو محو أو تغيير أو تعديل أو استرجاع أو استنباط البيانات والمعلومات الإلكترونية، وذلك باستخدام أي وسيط من الوسائط أو الحاسبات أو الأجهزة الأخرى الإلكترونية أو المغناطيسية أو الضوئية أو ما يُستحدث من تقنيات أو وسائط أخرى.

والمحتوى هو أى بيانات تؤدي بذاتها أو مجتمعة مع بيانات أو معلومات أخرى إلى تكوين معلومة أو تحديد توجه أو اتجاه أو تصور أو معني أو إشارة إلى بيانات أخرى^(١).

(١) المادة الأولى من قانون مكافحة جرائم تقنية المعلومات.

المطلب الرابع

الجرائم المرتكبة من مدير الموقع

أولاً: جريمة إنشاء أو إدارة أو استخدام موقع أو حساب خاص على شبكة معلوماتية، يهدف ارتكاب أو تسهيل ارتكاب جريمة معاقب عليها قانوناً.

تتحقق هذه الجريمة بمجرد إنشاء أو إدارة أو استخدام موقع أو حساب خاص على شبكة معلوماتية، بهدف ارتكاب أو تسهيل ارتكاب جريمة معاقب عليها قانوناً. حتى ولو لم تتحقق هذه الجريمة الأخيرة.

ويستوى أن تكون الجريمة التي يهدف الجاني إلى ارتكابها أو تسهيل ارتكابها معاقباً عليها في قانون مكافحة جرائم تقنية المعلومات، أو أى قانون آخر.

وقد أكدت المادة ٢٧ من قانون مكافحة جرائم تقنية المعلومات على ذلك، بقولها " يعاقب بالحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن مائة ألف جنيه، ولا تزيد عن ثلاثمائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من أنشا أو أدار أو استخدم موقعاً أو حساباً خاصاً على شبكة معلوماتية يهدف إلى ارتكاب أو تسهيل ارتكاب جريمة معاقب عليها قانوناً."

ثانياً: جريمة إخفاء أو العبث بالأدلة الرقمية لإحدى الجرائم المنصوص عليها في قانون مكافحة جرائم تقنية المعلومات.

جرم المشرع أفعال الإخفاء أو العبث بالأدلة الرقمية لإحدى الجرائم المنصوص عليها في قانون مكافحة جرائم تقنية المعلومات، التي يقوم بها كل مسئول عن إدارة موقع أو حساب خاص أو بريد إلكترونى أو نظام معلوماتى، والتي تقع على موقع أو حساب أو بريد إلكترونى بقصد إعاقة عمل الجهات الرسمية.

حيث قررت المادة ٢٨ من القانون بأنه " يعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن عشرين ألف جنيه ولا تجاوز مائتى ألف جنيه، أو بإحدى

هاتين العقوبتين، كل مسئول عن إدارة موقع أو حساب خاص أو بريد إلكتروني أو نظام معلوماتي إذا أخفى أو عبث بالأدلة الرقمية لإحدى الجرائم المنصوص عليها في هذا القانون والتي وقعت على موقع أو حساب أو بريد إلكتروني بقصد إعاقة عمل الجهات الرسمية المختصة".

ويقصد بالدليل الرقمي، أى معلومات إلكترونية لها قوة أو قيمة ثبوتية مخزنة أو منقولة أو مستخرجة أو مأخوذة من أجهزة الحاسب أو الشبكات المعلوماتية وما في حكمها، ويمكن تجميعها وتحليلها باستخدام أجهزة أو برامج أو تطبيقات تكنولوجية خاصة^(١).

ثالثاً: جريمة تعريض المسئول عن إدارة موقع أو حساب خاص أو بريد إلكتروني أو نظام معلوماتي، لإحدى الجرائم المنصوص عليها في قانون مكافحة جرائم تقنية المعلومات.

فكل مسئول عن إدارة الموقع أو الحساب الخاص أو البريد الإلكتروني أو النظام المعلوماتي عرض أي منهم لإحدى الجرائم المنصوص عليها في هذا القانون يعاقب بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن عشرين ألف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين^(٢).

والمقصود بالمسئول عن إدارة الموقع - أو الحساب الخاص أو البريد الإلكتروني أو النظام المعلوماتي - كل شخص مسئول عن تنظيم أو إدارة أو متابعة أو الحفاظ على موقع أو أكثر على الشبكة المعلوماتية، بما في ذلك حقوق الوصول لمختلف المستخدمين على ذلك الموقع أو تصميمه، أو توليد وتنظيم صفحاته أو محتواه أو المسئول عنه^(٣).

(١) المادة الأولى من قانون مكافحة جرائم تقنية المعلومات.

(٢) المادة ١/٢٩ من قانون مكافحة جرائم تقنية المعلومات.

(٣) المادة الأولى من قانون مكافحة جرائم تقنية المعلومات.

رابعاً: جريمة التسبب بالإهمال فى تعريض موقع أو حساب خاص أو بريد إلكترونى أو نظام معلوماتى، لإحدى الجرائم المنصوص عليها فى قانون مكافحة جرائم تقنية المعلومات.

تقع هذه الجريمة بمجرد تسبب المسئول عن إدارة الموقع أو الحساب الخاص أو البريد الإلكتروني أو النظام المعلوماتى، بإهماله فى تعرض أى منها لإحدى الجرائم المنصوص عليها فى قانون مكافحة جرائم تقنية المعلومات، ويشترط أن يكون ذلك الإهمال راجعاً إلى عدم اتخاذ التدابير والاحتياطات التأمينية الواردة فى اللائحة التنفيذية لهذا القانون.

حيث قررت المادة ٢/٢١ من قانون مكافحة جرائم تقنية المعلومات بأنه " يعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل مسئول عن إدارة الموقع أو الحساب الخاص أو البريد الإلكتروني أو النظام المعلوماتى تسبب بإهماله فى تعرض أى منهم لإحدى الجرائم المنصوص عليها فى هذا القانون، وكان ذلك بعدم اتخاذه التدابير والاحتياطات التأمينية الواردة فى اللائحة التنفيذية لقانون مكافحة جرائم تقنية المعلومات".

ويستلزم المشرع فى الجرائم الواردة بالبنود ثانياً، وثالثاً، ورابعاً توافر صفة معينة فى مرتكبها، أى شرط مفترض للجريمة لا يتصور قيامها بدون هذه الصفة، وهى أن يكون مرتكب هذه الجرائم مسئولاً عن إدارة الموقع أو الحساب الخاص أو البريد الإلكتروني أو النظام المعلوماتى، على حسب الأحوال.

فهذه الجرائم لا يمكن لأى شخص أن يرتكبها، فهى لا تقع إلا من الشخص الذى توافرت فيه هذه الصفة المحددة وقت ارتكاب الجريمة^(١).

(١) د/ عبد العظيم مرسى وزير، الشروط المفترضة فى الجريمة، دراسة تحليلية تأصيلية، دار النهضة العربية، ١٩٨٣، ص ٧١ وما بعدها.

المطلب الخامس

جرائم مقدمى الخدمة

يقصد بمقدم الخدمة أى شخص طبيعى أو اعتبارى يزود المستخدمين بخدمات تقنيات المعلومات والاتصالات، ويشمل ذلك من يقوم بمعالجة أو تخزين المعلومات بذاته أو من ينوب عنه في أى من تلك الخدمات أو تقنية المعلومات.

وقد جاء الفصل الخامس من قانون مكافحة جرائم تقنية المعلومات تحت عنوان " المسؤولية الجنائية لمقدمى الخدمة، وأورد العديد من الجرائم التى تقع من مقدمى الخدمة، وذلك على النحو التالى:

أولاً: جريمة الامتناع عن تنفيذ القرار الصادر من المحكمة الجنائية بحجب أحد المواقع أو الروابط.

تقع هذه الجريمة من كل مقدم خدمة امتنع عن تنفيذ القرار الصادر من المحكمة الجنائية المختصة بحجب أحد المواقع أو الروابط التى تُبث من داخل مصر أو خارجها، يضع أى عبارات أو أرقام أو صور أو أفلام أو أى مواد دعائية أو ما فى حكمها، ويشكل جريمة من الجرائم المنصوص عليها فى قانون مكافحة جرائم تقنية المعلومات.

ويشترط أن تشكل الأفعال السابقة - أو أى منها - تهديداً للأمن القومى أو تعريض أمن البلاد أو اقتصادها للخطر.

حيث قررت المادة ٣٠ من قانون جرائم تقنية المعلومات بأنه " يعاقب بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن خمسمائة ألف جنيه ولا تجاوز مليون جنيه، أو بإحدى هاتين العقوبتين، كل مقدم خدمة امتنع عن تنفيذ القرار الصادر من المحكمة

الجنائية المختصة بحجب أحد المواقع أو الروابط أو المحتوى المُشار إليه في الفقرة الأولى من المادة ٧ من هذا القانون" (١).

حالتى التشديد:

تصبح الجريمة جنائية، إذا ترتب على الامتناع عن تنفيذ القرار الصادر من المحكمة بحجب أحد المواقع، وفاة شخص أو أكثر، أو الإضرار بالأمن القومى.

والمقصود بالأمن القومى، كل ما يتصل باستقلال واستقرار وأمن الوطن ووحدته وسلامة أراضيه، وما يتعلق بشئون رئاسة الجمهورية ومجلس الدفاع الوطنى ومجلس الأمن القومى، ووزارة الدفاع والإنتاج الحربى، ووزارة الداخلية، والمخابرات العامة، وهيئة الرقابة الإدارية، والأجهزة التابعة لتلك الجهات (٢).

وتكون العقوبة السجن المشدد، والغرامة التى لا تقل عن ثلاثة ملايين جنيه ولا تجاوز عشرين مليون جنيه، وإلغاء ترخيص مزاوله النشاط.

ثانياً: جريمة إفشاء مقدم الخدمة للبيانات المحفوظة أو المخزنة.

يلتزم كل مقدم خدمة بالمحافظة على سرية البيانات التى تم حفظها وتخزينها (٣). ويعاقب مقدم الخدمة الذى يخالف هذا الالتزام - بالمحافظة على السرية - بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن خمسة آلاف جنيه ولا تجاوز عشرين ألف جنيه، أو

(١) تقرر المادة ٧ من قانون مكافحة جرائم تقنية المعلومات بأنه " لجهة التحقيق المختصة متى قامت أدلة على قيام موقع يُبث من داخل الدولة أو خارجها، بوضع أي عبارات أو أرقام أو صور أو أفلام أو أى مواد دعائية، أو ما في حكمها، مما يعد جريمة من الجرائم المنصوص عليها فى هذا القانون، ويشكل تهديداً للأمن القومى أو يعرض أمن البلاد أو اقتصادها القومى للخطر، أن تأمر بحجب الموقع أو المواقع محل البث، كلما أمكن تحقيق ذلك فنياً. وعلي جهة التحقيق عرض أمر الحجب على المحكمة المختصة، منعقدة في غرفة المشورة، خلال أربع وعشرين ساعة مشفوعاً بمذكرة برأيها، وتصدر المحكمة قرارها في الأمر مسبباً إما بالقبول أو بالرفض، في مدة لا تجاوز اثنين وسبعين ساعة من وقت عرضه عليها".

(٢) المادة الأولى من قانون مكافحة جرائم تقنية المعلومات.

(٣) وفقاً للمادة الثانية من قانون مكافحة جرائم تقنية المعلومات، تتمثل البيانات التى يلتزم مقدمو الخدمات بحفظها وتخزينها، والمحافظة على سريتها فيما يلى: أ- البيانات التى تمكن من التعرف على مستخدم الخدمة. ب- البيانات المتعلقة بمحتوي ومضمون النظام المعلوماتى المتعامل متى كانت تحت سيطرة مقدم الخدمة. ج- البيانات المتعلقة بحركة الاتصال. د- البيانات المتعلقة بالأجهزة الطرفية للاتصال. هـ- أي بيانات أخرى يصدر بتحديددها قرار من مجلس إدارة الجهاز القومى لتنظيم الاتصالات.

بإحدى هاتين العقوبتين. وتتعدد عقوبة الغرامة بتعدد المجنى عليهم من مستخدمي الخدمة^(١).

ويقصد بمستخدم الخدمة، كل شخص طبيعي أو اعتباري، يستعمل خدمات تقنية المعلومات، أو يستفيد منها بأي صورة كانت^(٢).

ثالثاً: جريمة إفشاء أو إفصاح مقدم الخدمة عن البيانات المحفوظة أو المخزنة بغير أمر مسبب، من إحدى الجهات القضائية المختصة.

يلتزم مقدمو الخدمة - وفقاً للمادة الثانية من قانون مكافحة جرائم تقنية المعلومات - بعدم الإفصاح، عن البيانات المحفوظة أو المخزنة.

ويعاقب مقدم الخدمة الذي يفصح بغير أمر مسبب، من إحدى الجهات القضائية المختصة، عن البيانات المحفوظة أو المخزنة، بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن خمسة آلاف جنيه ولا تجاوز عشرين ألف جنيه، أو بإحدى هاتين العقوبتين.

وتتعدد عقوبة الغرامة بتعدد المجنى عليهم من مستخدمي الخدمة^(٣).

رابعاً: جريمة امتناع مقدم خدمة عن تنفيذ قرار جهة التحقيق بتسليم ما لديه من بيانات أو معلومات.

يلتزم مقدم الخدمة بتسليم ما لديه من بيانات أو معلومات تتعلق بنظام معلوماتي أو جهاز تقني موجود تحت سيطرته أو مخزنة لديه، وكذا بيانات مستخدمي خدمته وحركة الاتصالات التي تمت على ذلك النظام أو النظام التقني^(٤)، وذلك بناء على القرار الصادر بذلك من جهة التحقيق المختصة.

(١) المادة ٣١ من قانون مكافحة جرائم تقنية المعلومات.

(٢) المادة الأولى من قانون مكافحة جرائم تقنية المعلومات.

(٣) المادة ٣١ من قانون مكافحة جرائم تقنية المعلومات.

(٤) المادة ٣/٦ من قانون مكافحة جرائم تقنية المعلومات.

ويعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن عشرين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل مقدم خدمة امتنع عن تنفيذ القرار الصادر من جهة التحقيق المختصة بتسليم ما لديه من البيانات أو المعلومات الواردة بقرار جهة التحقيق المختصة^(١).

خامساً: جريمة امتناع مقدم الخدمة عن حفظ وتخزين سجل النظام المعلوماتي أو أى وسيلة لتقنية المعلومات.

كما يلتزم مقدم الخدمة - أيضاً - بحفظ وتخزين سجل النظام المعلوماتي أو أى وسيلة لتقنية المعلومات، لمدة مائة وثمانين يوماً متصلة.

ويعاقب مقدم الخدمة إذا أخل بأى من هذه الالتزامات بغرامة لا تقل عن خمسة ملايين جنيه ولا تجاوز عشرة ملايين جنيه، وتضاعف عقوبة الغرامة فى حالة العود، وللمحكمة أن تقضى بإلغاء الترخيص الصادر لمقدم الخدمة^(٢).

سادساً: جريمة عدم توفير مقدم الخدمة البيانات والمعلومات لمستخدمى خدماته.

يجب على مقدم الخدمة - طبقاً للفقرة ثانياً من المادة الثانية من قانون مكافحة جرائم تقنية المعلومات - أن يوفر لمستخدمى خدماته ولأى جهة حكومية مختصة، بالشكل والطريقة التى يمكن الوصول إليها بطريقة ميسرة ومباشرة ومستمرة، البيانات والمعلومات الآتية:

- ١- اسم مقدم الخدمة وعنوانه.
- ٢- معلومات الاتصال المتعلقة بمقدم الخدمة، بما فى ذلك عنوان الاتصال الإلكتروني.
- ٣- بيانات الترخيص لتحديد هوية مقدم الخدمة، وتحديد الجهة المختصة التى يخضع لإشرافها.
- ٤- أى معلومات أخرى يقدر الجهاز أهميتها لحماية مستخدمى الخدمة، ويصدر بتحديدتها قرار من وزير الاتصالات وتكنولوجيا المعلومات.

(١) المادة ٣٢ من قانون مكافحة جرائم تقنية المعلومات.

(٢) المادة ١/٣٣ من قانون مكافحة جرائم تقنية المعلومات.

ويعاقب مقدم الخدمة - ممن لا يوفر لمستخدمي خدماته تلك البيانات والمعلومات - بغرامة لا تقل عن عشرين ألف جنيه ولا تجاوز مائتي ألف جنيه^(١).
سابعاً: جريمة عدم حصول مقدمي الخدمة على بيانات المستخدمين.

وفقاً للبند رابعاً من المادة الثانية من قانون مكافحة جرائم تقنية المعلومات، يلتزم مقدمو خدمات تقنية المعلومات ووكلائهم وموزعوهم التابعون لهم المنوط بهم تسويق تلك الخدمات بالحصول على بيانات المستخدمين، ويُحظر على غيرهم القيام بذلك. ويعاقب كل مقدم خدمة خالف هذا الالتزام، بغرامة لا تقل عن عشرين ألف جنيه ولا تجاوز مائتي ألف جنيه^(٢).

ثامناً: جريمة عدم التزام مقدمو الخدمة بتوفير كافة الإمكانيات لجهات الأمن القومي بما يمكنها من ممارسة اختصاصاتها.

يلتزم مقدمو الخدمة - وفقاً للفقرة ثانياً من المادة الثانية من قانون مكافحة جرائم تقنية المعلومات - بأن يوفر لجهات الأمن القومي - ووفقاً لاحتياجها - كافة الإمكانيات الفنية التي تتيح لتلك الجهات ممارسة اختصاصاتها وفقاً للقانون، وذلك بناء على طلب تلك الجهات.

وحدد المشرع - في المادة الأولى من قانون مكافحة جرائم تقنية المعلومات - جهات الأمن القومي بأنها: رئاسة الجمهورية، ووزارة الدفاع، ووزارة الداخلية، والمخابرات العامة، وهيئة الرقابة الإدارية.

ويعاقب كل مقدم خدمة - خالف ذلك الالتزام - بالحبس مدة لا تقل عن ثلاثة أشهر، وبالغرامة التي لا تقل عن مائتي ألف جنيه ولا تجاوز مليون جنيه^(٣).

(١) ، المادة ٢/٣٣ من قانون مكافحة جرائم تقنية المعلومات.

(٣) المادة ٣/٣٣ من قانون مكافحة جرائم تقنية المعلومات.

المبحث الثانى

الأحكام الإجرائية

لمكافحة الجرائم الإلكترونية

أولاً: منح صفة الضبطية القضائية للعاملين بالجهاز القومى لتنظيم الاتصالات.

يجوز بقرار من وزير العدل - بالاتفاق مع وزير الاتصالات وتكنولوجيا المعلومات - منح صفة الضبطية القضائية للعاملين بالجهاز القومى لتنظيم الاتصالات، أو غيرهم ممن تحددهم جهات الأمن القومى بالنسبة للجرائم التى تقع بالمخالفة لأحكام قانون مكافحة جرائم تقنية المعلومات، والمتعلقة بأعمال وظائفهم^(١).

ويقصد بجهات الأمن القومى: رئاسة الجمهورية، ووزارة الدفاع، ووزارة الداخلية، والمخابرات العامة، وهيئة الرقابة الإدارية.

ثانياً: إصدار جهة التحقيق أمراً مسبباً لمأمورى الضبط القضائى لاتخاذ بعض الإجراءات.

يكون لجهة التحقيق المختصة، أن تصدر أمراً مسبباً لمأمورى الضبط القضائى، للقيام بإجراء أو أكثر من الإجراءات التالية:

١- ضبط أو سحب أو جمع أو التحفظ على البيانات والمعلومات أو أنظمة المعلومات أو تتبعها فى أى مكان أو نظام أو برنامج أو دعامة إلكترونية أو حاسب تكون موجودة فيه.

(١) المادة ٥ من قانون مكافحة جرائم تقنية المعلومات.

ويتم تسليم أدلتها الرقمية^(١) للجهة مصدرة الأمر، وذلك بشرط ألا يؤثر ذلك على استمرارية النظم وتقديم الخدمة.

٢- البحث والتفتيش والدخول والنفوذ إلى برامج الحاسب وقواعد البيانات وغيرها من الأجهزة والنظم المعلوماتية تحقيقاً لغرض الضبط.

٣- أمر مقدم الخدمة^(٢) بتسليم ما لديه من بيانات أو معلومات تتعلق بنظام معلوماتي أو جهاز تقني موجودة تحت سيطرته أو مخزنة لديه، فضلاً عن بيانات مستخدمى خدمته وحركة الاتصالات التي تمت على ذلك النظام أو النظام التقني^(٣).

شروط الأمر الصادر من جهة التحقيق:

يشترط في الأمر الصادر من جهة التحقيق لمأمور الضبط القضائي - باتخاذ إجراء أو أكثر من الإجراءات السابقة - توافر الشرطين التاليين:

الشرط الأول: أن يكون الأمر مسبباً.

الشرط الثاني: أن يكون لذلك فائدة في ظهور الحقيقة على ارتكاب جريمة من الجرائم المعاقب عليها بمقتضى قانون مكافحة جرائم تقنية المعلومات.

استئناف أوامر جهة التحقيق:

يكون استئناف أى من الأوامر السابقة - الصادرة من جهة التحقيق - أمام المحكمة الجنائية المختصة، منعقدة في غرفة المشورة، خلال المواعيد، ووفقاً للإجراءات المقررة في قانون الإجراءات الجنائية.

(١) الدليل الرقمي هو أى معلومات إلكترونية لها قوة أو قيمة ثبوتية مخزنة أو منقولة أو مستخرجة أو مأخوذة من أجهزة الحاسب أو الشبكات المعلوماتية وما فى حكمها، ويمكن تجميعها وتحليلها باستخدام أجهزة أو برامج أو تقنيات تكنولوجية خاصة. (المادة الأولى من قانون مكافحة جرائم تقنية المعلومات)

(٢) مقدم الخدمة هو أى شخص طبيعى أو اعتبارى يزود المستخدمين بخدمات تقنيات المعلومات والاتصالات، ويشمل ذلك من يقوم بمعالجة أو تخزين المعلومات بذاته أو من ينوب عنه فى أى من تلك الخدمات أو تقنيات المعلومات. (المادة الأولى من قانون مكافحة جرائم تقنية المعلومات)

(٣) المادة ٦ من قانون مكافحة جرائم تقنية المعلومات.

ثالثاً: الأمر بحجب الموقع محل جريمة من الجرائم الواردة بقانون مكافحة جرائم تقنية المعلومات.

يكون لجهة التحقيق متى قامت أدلة على قيام موقع - يُبث من داخل مصر أو خارجها - بوضع عبارات أو أرقام أو صور أو أفلام أو مواد دعائية - أو ما فى حكمها - يعد جريمة من الجرائم المنصوص عليها فى قانون مكافحة جرائم تقنية المعلومات، ويشكل تهديداً للأمن القومى أو يعرض أمن البلاد أو اقتصادها القومى للخطر، أن تأمر بحجب الموقع أو المواقع محل البث، كلما أمكن تحقيق ذلك^(١).

١- شروط أمر الحجب:

يشترط لصدور أمر الحجب، أن تشكل أى من تلك الأفعال تهديداً للأمن القومى أو يعرض أمن البلاد أو اقتصادها القومى للخطر، وإمكانية تحقيق ذلك الحجب من الناحية التقنية.

٢- عرض أمر الحجب على المحكمة المختصة:

يتعين على جهة التحقيق عرض أمر حجب الموقع - أو المواقع محل البث - على المحكمة المختصة - منعقدة فى غرفة المشورة - خلال أربع وعشرين ساعة مشفوعاً بمذكرة برأيها.

٣- جواز إبلاغ الجهاز القومى لتنظيم الاتصالات للقيام بإخطار مقدم الخدمة بالحجب المؤقت للموقع.

يجوز فى حالة الاستعجال، قيام جهات التحرى والضبط المختصة، بإبلاغ الجهاز القومى لتنظيم الاتصالات، ليقوم بإخطار مقدم الخدمة على الفور بالحجب المؤقت للموقع أو المحتوى أو المواقع أو الروابط محل الجريمة، ويلتزم مقدم الخدمة بتنفيذ مضمون الإخطار فور وروده إليه.

(١) المادة ٧ من قانون مكافحة جرائم تقنية المعلومات.

٤- شروط الإخطار بالحجب المؤقت للموقع:

- أ- توافر حالة الاستعجال لوجود خطر حال، أو ضرر وشيك الوقوع.
- ب- صدور الإخطار بالحجب المؤقت من الجهاز القومى لتنظيم الاتصالات بناء على بلاغ من جهات التحرى والضبط المختصة.
- ج- تحرير جهات التحرى والضبط لمحضر يثبت فيه ما تم من إجراءات يعرض على جهات التحقيق خلال ثمان وأربعين ساعة من تاريخ الإبلاغ للجهاز.

٥- اعتبار الحجب المؤقت كأن لم يكن:

إذا لم يعرض المحضر المحرر بمعرفة جهات التحرى والضبط على جهات التحقيق خلال المواعيد المقررة، يعد الحجب الذى تم كأن لم يكن.

٦- سلطة محكمة الموضوع فى إلغاء قرار الحجب أو تعديل نطاقه:

لمحكمة الموضوع أثناء نظر الدعوى، أو بناء على طلب جهة التحقيق أو الجهاز القومى لتنظيم الاتصالات، أو ذوى الشأن، أن تأمر بإنهاء القرار الصادر بالحجب المؤقت، أو تعديل نطاقه.

٧- سقوط أمر الحجب المؤقت:

يسقط الأمر الصادر بالحجب المؤقت فى حالتين: الحالة الأولى: صدور أمر بالألا وجه لإقامة الدعوى الجنائية، والحالة الثانية: صدور حكم نهائى بالبراءة.

٨- التظلم من قرارات حجب الموقع:

لكل من صدر ضده قرار بالحجب، و للنيابة العامة ولجهة التحقيق المختصة، ولكل ذى شأن، التظلم من ذلك القرار، أو إجراءات تنفيذه أمام محكمة الجنايات المختصة، وذلك بعد انقضاء سبعة أيام من تاريخ صدور الأمر، أو من تاريخ تنفيذه حسب الأحوال.

وفى حالة رفض التظلم، يجوز للنياحة العامة أو جهة التحقيق المختصة، أو ذوى الشأن التقدم بطلب جديد، كلما انقضت ثلاثة أشهر من تاريخ الحكم برفض التظلم.

ويكون التظلم بتقرير يودع قلم كتاب محكمة الجنايات المختصة، ويحدد رئيس المحكمة جلسة لنظر التظلم، يُعلن بها المتظلم والجهاز القومى لتنظيم الاتصالات، وكل ذى شأن.

ويجب على المحكمة أن تفصل فى التظلم خلال مدة لا تتجاوز سبعة أيام من تاريخ التقرير بالتظلم.

وهذا الميعاد ميعاد تنظيمى لا يترتب على مخالفته أى جزاء إجرائى^(١).

رابعاً: الأمر بالمنع من السفر أو الوضع على قوائم ترقيب الوصول.

يجوز للنائب العام أو من يفوضه من المحامين العموم الأول بنيايات الاستئناف، ولجهات التحقيق المختصة، عند الضرورة، أو عند وجود أدلة كافية على جدية الاتهام فى ارتكاب جريمة من الجرائم المنصوص عليها فى قانون مكافحة جرائم تقنية المعلومات أو الشروع فى ارتكابها، أن يأمر بمنع المتهم من السفر، أو بوضع اسمه على قوائم ترقيب الوصول، وذلك بأمر مسبب لمدة محددة^(٢).

١- شروط صدور الأمر بالمنع من السفر أو الوضع على قوائم ترقيب الوصول:

يشترط لصحة الأمر بالمنع من السفر أو الوضع على قوائم ترقيب الوصول، الشروط التالية:

الشرط الأول: صدور القرار من النائب العام أو من يفوضه من المحامين العموم الأول بنيايات الاستئناف، أو جهات التحقيق المختصة.

الشرط الثانى: توافر حالة من حالات الضرورة.

(١) نقض جنائى جلسة ٩ يناير ١٩٩٧، مجموعة أحكام محكمة النقض، س ٤٨ رقم ٨، ص ٥٩؛ الطعن رقم ١ لسنة ٢٠١٧ كيانات إرهابية، جلسة ٢٠/٥/٢٠١٧، لم ينشر بعد.

(٢) المادة ٩ من قانون مكافحة جرائم تقنية المعلومات.

الشرط الثالث: وجود أدلة كافية على جدية الاتهام فى ارتكاب جريمة من الجرائم المنصوص عليها فى قانون مكافحة جرائم تقنية المعلومات أو الشروع فيها.
الشرط الرابع: تسبب الأمر بالمنع من السفر أو الوضع على قوائم ترقيب الوصول.
الشرط الخامس: تحديد مدة الأمر.

٢- التظلم من الأمر بالمنع من السفر:

يجوز لمن صدر ضده أمر المنع من السفر أن يتظلم من هذا الأمر أمام محكمة الجنايات المختصة، خلال خمسة عشر يوماً من تاريخ علمه به. وفى حالة رفض التظلم، يكون لمن صدر ضده الأمر، أن يقوم بتظلم جديد كلما انقضت ثلاثة أشهر من تاريخ الحكم برفض التظلم. ويكون التظلم بتقرير يودع فى قلم كتاب محكمة الجنايات المختصة، ويحدد رئيس المحكمة جلسة لنظر التظلم، تُعلن بها النيابة العامة والمتظلم. وتفصل المحكمة فى التظلم خلال خمسة عشر يوماً من تاريخ التقرير به^(١)، بحكم مسبب، وذلك بعد سماع أقوال المتظلم والنيابة العامة أو جهة التحقيق حسب الأحوال. وللمحكمة - فى سبيل نظر التظلم - أن تتخذ ما تراه من إجراءات أو تحقيقات ترى لزومها فى هذا الشأن.

٣- العدول عن التعديل فى أمر المنع من السفر أو ترقيب الوصول:

يجوز للنيابة العامة وجهات التحقيق المختصة فى كل وقت العدول عن الأمر الصادر منها، كما يجوز لها التعديل فيه برفع الاسم من قوائم المنع من السفر أو ترقيب الوصول لمدة محددة، إذا دعت الحاجة إلى ذلك.

٤- إنهاء الأمر بالمنع من السفر:

- ينتهى الأمر بالمنع من السفر فى ثلاث حالات - أيهما أقرب - هى:
- أ- مرور سنة من تاريخ صدور الأمر بالمنع من السفر.
 - ب- صدور قرار بالألا وجه لإقامة الدعوى الجنائية.
 - ج- صدور حكم نهائى بالبراءة.

(١) وهذا الميعاد تنظيمى لا يترتب على مخالفته أى جزاء إجرائى.

المبحث الثالث

نطاق تطبيق قانون مكافحة جرائم تقنية المعلومات

من حيث المكان

تقرر المادة (٣) من قانون مكافحة جرائم تقنية المعلومات، بأنه " مع عدم الإخلال بأحكام الباب الأول من الكتاب الأول من قانون العقوبات، تسري أحكام هذا القانون على كل من ارتكب خارج جمهورية مصر العربية من غير المصريين جريمة من الجرائم المنصوص عليها في هذا القانون، متي كان الفعل معاقباً عليه في الدولة التي وقع فيها تحت أي وصف قانوني، وذلك في أي من الأحوال الآتية :

١- إذا ارتكبت الجريمة على متن أي وسيلة من وسائل النقل الجوي أو البري أو المائي، وكانت مسجلة لدى جمهورية مصر العربية أو تحمل علمها.

٢- إذا كان المجني عليهم أو أحدهم مصرياً.

٣- إذا تم الإعداد للجريمة أو التخطيط أو التوجيه أو الإشراف عليها أو تمويلها في جمهورية مصر العربية.

٤- إذا ارتكبت الجريمة بواسطة جماعة إجرامية منظمة، تمارس أنشطة إجرامية في أكثر من دولة من بينها جمهورية مصر العربية.

٥- إذا كان من شأن الجريمة إلحاق ضرر بأى من مواطني جمهورية مصر العربية أو المقيمين فيها، أو بأمنها أو بأى من مصالحها، فى الداخل أو الخارج.

٦- إذا وُجد مرتكب الجريمة فى جمهورية مصر العربية، بعد ارتكابها ولم يتم تسليمه."

فيُطبَّق قانون مكافحة جرائم تقنية المعلومات خارج الحدود - ولو كانت الجريمة المنصوص عليها فيه - قد وقعت فى ظل تشريع أجنبى، وحالات امتداد الاختصاص القضائى المصرى هى:

(أ) إذا ارتكبت الجريمة على متن وسيلة من وسائل النقل الجوي أو البري أو

المائى وكانت مسجلة لدى جمهورية مصر العربية أو تحمل علمها.

(ب) إذا كان المجني عليهم أو أحدهم مصرياً.

(ج) إذا تم الإعداد للجريمة أو التخطيط أو التوجيه أو الإشراف عليها أو تمويلها

في جمهورية مصر العربية.

(د) إذا ارتكبت الجريمة بواسطة جماعة إجرامية منظمة تمارس أنشطة إجرامية في أكثر من دولة من بينها جمهورية مصر العربية.

(هـ) إذا كان من شأن الجريمة إلحاق ضرر بأي من مواطني جمهورية مصر العربية أو المقيمين فيها، أو بأمنها، أو بأي من مصالحها في الداخل أو الخارج.

(و) إذا وُجد مرتكب الجريمة في جمهورية مصر العربية، بعد ارتكابها ولم يتم تسليمه.

مع ملاحظة أنه يشترط لامتداد الاختصاص القضائي المصرى فى هذه الحالات توافر شرطين هما: أن يكون مرتكب الجريمة من غير المصريين، وأن يكون الفعل معاقباً عليه فى الدولة التى وقع فيها تحت أى وصف قانونى.

أما إذا ارتكب المصرى جريمة - من الجرائم المنصوص عليها فى هذا القانون - فى الخارج، فيشترط لمحاكمته أن يعود إلى مصر وأن يكون الفعل معاقباً عليه بمقتضى قانون البلد الذى ارتكب فيه. وهو ما يعرف بمبدأ الشخصية الإيجابية^(١).

وهدياً بما تقدم فسوف نعرض لنطاق تطبيق قانون مكافحة جرائم تقنية المعلومات - من حيث المكان - وذلك من خلال أربعة مطالب على النحو التالى:

المطلب الأول: مبدأ إقليمية قانون مكافحة جرائم تقنية المعلومات.

المطلب الثانى: مبدأ الشخصية السلبية فى قانون مكافحة جرائم تقنية المعلومات.

المطلب الثالث: مبدأ عينية قانون مكافحة جرائم تقنية المعلومات.

المطلب الرابع: مبدأ الاختصاص الجنائى العالمى فى قانون مكافحة جرائم تقنية المعلومات.

المطلب الخامس: شروط اختصاص السلطات المصرية بجرائم تقنية المعلومات المرتكبة فى الخارج.

(١) تقرر المادة (٣) من قانون العقوبات بأنه "كل مصرى ارتكب وهو فى خارج القطر فعلاً يعتبر جنائياً أو جنحة فى هذا القانون يعاقب بمقتضى أحكامه إذا عاد إلى القطر وكان الفعل معاقباً عليه بمقتضى قانون البلد الذى ارتكبه فيه".

المطلب الأول

مبدأ إقليمية قانون مكافحة جرائم تقنية المعلومات

١- ماهية مبدأ الإقليمية:

يعنى مبدأ الإقليمية أن قانون مكافحة جرائم تقنية المعلومات هو القانون الواجب التطبيق بشأن أية جريمة من الجرائم المنصوص عليها فيه. ذلك أن قانون البلد الذى وقعت فيه الجريمة يسرى على الجرائم التى تقع على إقليم تباشر الدولة سيادتها عليه. فالقانون المصرى هو الذى يسرى على أية جريمة ترتكب على إقليم هذه الدولة أياً كانت جنسية المتهم، وأياً كانت جنسية المجنى عليه، وسواء وقعت الجريمة ضد مصالح مصر أو ضد دولة غيرها.

ولذلك فإن تطبيق قانون مكافحة جرائم تقنية المعلومات يقتضى الالتزام بالقواعد

الآتية:-

(أ) عند وقوع فعل على الإقليم المصرى، فإنه يجب الرجوع إلى القانون المصرى لمعرفة ما إذا كان الفعل المرتكب يعد جريمة والعقوبة المقررة له، فإن كان الفعل يعد جريمة فعلى القاضى أن يطبق على مرتكب الجريمة العقوبة المقررة فى هذا القانون.

(ب) عدم تطبيق قواعد أى قانون أجنبى على جريمة من الجرائم الواردة بقانون مكافحة جرائم تقنية المعلومات وقعت على الإقليم المصرى. فإذا وقعت جريمة من هذه الجرائم على إقليم مصر فلا يجوز تطبيق أى قانون خلاف القانون المصرى أياً كان مرتكبها أو المجنى عليه فيها، وأياً كانت المصلحة المضارة من ارتكاب الجريمة.

٢- التوسع فى مبدأ الإقليمية:

يعنى مبدأ الإقليمية أن القانون الوطنى ينطبق على كافة الجرائم التى ترتكب على إقليم الدولة سواء كان الجانى أو المجنى عليه فيها وطنياً أو أجنبياً، وسواء أكانت الجريمة قد هدت مصالح الدولة صاحبة السيادة على الإقليم أو هدت مصالح دولة أجنبية.

ولم يضع المشرع المصرى تحديداً خاصاً لإقليم الدولة ومن ثم يتعين الرجوع إلى قواعد القانون الدولى العام لمعرفة المقصود به. وإقليم الدولة - طبقاً لقواعد القانون الدولى العام- يشمل الإقليم الأرضى والإقليم البحرى والإقليم الجوى.

ويقصد بالإقليم الأرضى تلك الأراضى التى تنتهى عند حدود الدولة السياسية مع البلاد المجاورة بما فيها الأنهار الداخلية وهى التى تباشر عليها الدولة سيادتها.

والإقليم البحرى للدولة هو المياه الإقليمية لها، أى جزء البحر العام الملاصق لشواطئ الدولة والذي يلزمها لتحقيق أغراضها الدفاعية والاقتصادية والصحية.

وأما الإقليم الجوى للدولة، فهو الأجواء الهوائية التى تعلو إقليمها الأرضى ومياهاها الإقليمية بغير حدود فى الارتفاع فتمتد سيادة الدولة إلى هذه الأجواء.

وقد توسع المشرع المصرى - فى القانون رقم ١٧٥ لسنة ٢٠١٨ فى شأن مكافحة جرائم تقنية المعلومات - فى تحديد المقصود بالإقليمية - فى نطاق تطبيق القانون - حيث قرر بسريان أحكام هذا القانون على كل مرتكب جريمة من الجرائم الواردة فى هذا القانون - من غير المصريين - إذا تم ارتكابها على متن وسيلة من وسائل النقل الجوى أو البرى أو المائى، متى كانت هذه الوسيلة مسجلة لدى جمهورية مصر العربية أو تحمل علمها.

المطلب الثانى

مبدأ الشخصية السلبية فى قانون مكافحة جرائم تقنية المعلومات

يُراد بمبدأ شخصية القانون صورتان:

صورة إيجابية: وهى تطبيق القانون الوطنى على الأفعال التى يرتكبها المواطنون فى الخارج، فمجرد تمتعه بجنسية الدولة يكفى لكى ينطبق على أفعاله قانون بلده أياً كان مكان ارتكابه لجرائمه.

وصورة سلبية: وهى تطبيق القانون الوطنى على الجرائم التى تقع اعتداءً على المواطنين فى الخارج أياً كانت جنسية المعتدى.

فالوجه السلبى لمبدأ شخصية القانون يعنى تطبيق القانون الوطنى على كل جريمة يكون المجنى عليه فيها وطنياً ولو كان مرتكب هذه الجريمة أجنبياً ارتكبها خارج إقليم الدولة.

وترجع العلة فى ذلك إلى رغبة الدولة فى حماية رعاياها إذا تعرضوا لاعتداء إجرامى وهم خارج إقليمها.

وقد أخذ المشرع المصرى فى القانون رقم ١٧٥ لسنة ٢٠١٨ - بشأن مكافحة جرائم تقنية المعلومات - بمبدأ الشخصية السلبية، وذلك بتطبيق أحكام ذلك القانون على من ارتكب خارج مصر - من غير المصريين - جريمة من الجرائم الواردة فى هذا القانون - متى كان الفعل معاقباً عليه فى الخارج تحت أى وصف قانونى - وذلك إذا كان المجنى عليهم أو أحدهم مصرياً.

وفى ذلك تقرر المادة الثالثة من القانون بأنه " ... تسري أحكام هذا القانون ... وذلك فى أى من الأحوال الآتية: ١- ... ٢- إذا كان المجنى عليهم أو أحدهم مصرياً".

المطلب الثالث

مبدأ عينية قانون مكافحة جرائم تقنية المعلومات

١- ماهية مبدأ العينية:

يعنى مبدأ العينية أن يطبق القانون الجنائي للدولة على الجرائم التي تهدد كيان الدولة وأمنها أو تمس مصالحها الجوهرية، وذلك بصرف النظر عن جنسية مرتكبها وكذا المكان الذي وقعت فيه^(١). حتى ولو لم تكن هذه الجريمة معاقباً عليها طبقاً لقانون الدولة التي ارتكبت فيها^(٢).

وتأتى أهمية مبدأ العينية، حيث تحرص الدول جميعها على بسط سلطاتها التشريعية على الجرائم الماسة بمصالحها الأساسية، وذلك في حالة عدم اهتمام الدولة التي وقعت هذه الجرائم على إقليمها، ذلك أنه قد يحدث ألا يطبق قانون هذه الدولة - لسبب أو لآخر - مما قد يترتب عليه إفلات الجاني من العقاب. ولذلك فإن الدولة بتقريرها مبدأ العينية تمارس نوعاً من الدفاع الشرعي عن مصالحها الأساسية^(٣).

٢- نطاق مبدأ العينية:

نظراً لأن الجرائم الإلكترونية من شأنها تهديد كيان الدولة وأمنها، فضلاً عن المساس بمصالحها الجوهرية، فلم يكن ثمة بُد من مواجهتها تشريعياً بكل الحسم ويسيف القانون وسلاح الشرعية، وذلك من خلال توسيع نطاق تطبيق قانون مكافحة جرائم تقنية المعلومات والأخذ بمبدأ العينية.

(١) د/ أحمد شوقي أبو خطوة، شرح الأحكام العامة لقانون العقوبات، دار النهضة العربية، ٢٠٠٥، ص ١١٤. وترجع علة هذا المبدأ إلى أن " هذه الجرائم لو ارتكبت خارج إقليم الدولة فليس من المؤكد أن تهتم الدولة التي ارتكبت الجرائم على إقليمها بملاحقة المتهم ومحاكمته عن تلك الجرائم".

(٢) د/ سليمان عبد المنعم، النظرية العامة لقانون العقوبات، ٢٠٠٩، ص ١٣٨.

(٣) R. MERLE et A. VITU, Procédure Pénale cujas, no 39, p.53.

إذا كان مبدأ إقليمية قانون العقوبات يقصر تطبيق قانون العقوبات على إقليم الدولة فإنه بذلك لا يحيط بالمصلحة العامة للدولة تماماً، إذ توجد جرائم ترتكب خارج إقليم الدولة ولكنها ذات خطر على الدولة وتقتضى المصلحة أن تخضع لحكم قانون العقوبات الوطني، فإخضاع هذه الجرائم لحكم القانون هو ما يسمى بمبدأ عينية قانون العقوبات بصرف النظر عن جنسية مرتكبها. د/ عبد الرؤوف مهدي، شرح القواعد العامة لقانون العقوبات، دار النهضة العربية، ٢٠٠٩، ص ١٤٣.

حيث يقرر البند الخامس من المادة (٣) من قانون مكافحة جرائم تقنية المعلومات بأنه " إذا كان من شأن الجريمة إلحاق ضرر بأى من مواطنى جمهورية مصر العربية، أو المقيمين فيها، أو بأمنها، أو بأى من مصالحها، فى الداخل أو الخارج".

وتعد هذه الحالات تطبيقاً لمبدأ عينية قانون العقوبات المصرى، حيث تقرر المادة ٢/ثانياً منه بسريان أحكام هذا القانون على " كل من ارتكب فى خارج القطر جريمة من الجرائم الآتية: (أ) جناية مخلة بأمن الحكومة مما نص عليه فى البابين الأول والثانى من الكتاب الثانى من هذا القانون. (ب) جناية تزوير مما نص عليه فى المادة ٢٠٦ من هذا القانون. (ج) جناية تقليد أو تزيف أو تزوير عملة ورقية أو معدنية مما نص عليه فى المادة ٢٠٢ أو جناية إدخال تلك العملة الورقية أو المعدنية المقلدة أو المزيفة أو المزورة إلى مصر أو إخراجها منها أو ترويجها أو حيازتها بقصد الترويج أو التعامل بها مما نص عليه فى المادة ٢٠٣ بشرط أن تكون العملة متداولة قانوناً فى مصر ".

المطلب الرابع

مبدأ الاختصاص الجنائي العالمي فى قانون مكافحة جرائم تقنية المعلومات.

١- ماهية الاختصاص الجنائي العالمي:

يقصد بالاختصاص الجنائي العالمي، أن تمتد كل دولة سلطان قانونها العقابى إلى كل أنحاء العالم، بأن يكون لكل دولة ولاية القضاء فى أية جريمة تنص عليها قوانينها الجنائية، وذلك بصرف النظر عن مكان ارتكاب الجريمة - سواء وقعت على إقليمها أو إقليم دولة أخرى - وبصرف النظر عن شخصية مرتكبها، بشرط أن يقبض على الجانى فى إقليم الدولة^(١).

فطبقاً لمبدأ الاختصاص الجنائي العالمي^(٢)، يجب تطبيق القانون الوطنى على كل جريمة يقبض على مرتكبها فى إقليم الدولة، وذلك بصرف النظر عن جنسية الجانى أو جنسية المجنى عليه أو مكان ارتكاب الجريمة، فطبقاً لهذا المبدأ يتحدد الاختصاص المكانى للقانون الوطنى بتواجد الجانى فى الدولة أو القبض عليه فيها.

فالاختصاص الجنائي العالمي يعنى صلاحية تقرر للقضاء الوطنى فى ملاحقة ومحاكمة وعقاب مرتكب أنواع معينة من الجرائم التى يحددها القانون الوطنى دون النظر لمكان ارتكابها، ودون اشتراط توافر ارتباط معين بين الدولة وبين مرتكبها أو ضحاياها، وأياً كانت جنسية مرتكبها أو ضحاياها.

(١) د/ طارق سرور، الاختصاص الجنائي العالمي، دار النهضة العربية، ٢٠٠٦؛ د/ كمال أنور محمد، تطبيق قانون العقوبات من حيث المكان، رسالة دكتوراه، كلية الحقوق جامعة القاهرة، ١٩٦٧، ص ١٥٩ وما بعدها.

(٢) يرى بعض الفقه تسمية مبدأ الاختصاص الجنائي العالمي بـ "مبدأ العالمية" د/ عبد الرؤوف مهدى، شرح القواعد العامة لقانون العقوبات، المرجع السابق، ص ١٥٣؛ د/ أحمد فتحى سرور، الوسيط فى قانون العقوبات، القسم العام، الطبعة السادسة، ١٩٩٩، ص ١١١. وأسماء البعض الآخر " مبدأ عالمية القاعدة الجنائية". د/ عبد العظيم وزير، شرح قانون العقوبات، القسم العام، ٢٠١٠، ص ١٠٢.

وفى ضوء ما تقدم يصبح تحديد نطاق إقليم الدولة أو تحديد مكان وقوع الجريمة أو النظر إلى جنسية مرتكب الجريمة أو جنسية ضحاياها غير ذى جدوى^(١).

وعلى ذلك يمنح الاختصاص الجنائى العالمى أجهزة الدولة سلطة ملاحقة مرتكبى جرائم معينة يحددها القانون الوطنى^(٢) - أياً كان مكان ارتكاب الجريمة - وتقديمه للمحاكمة بواسطة قضائه الوطنى الذى يكون له ولاية الفصل فى الدعوى^(٣)، دون تطلب صفة معينة تربطه بالدولة.

٢- مبررات مبدأ الاختصاص الجنائى العالمى:

ترجع مبررات الأخذ بمبدأ الاختصاص الجنائى العالمى فى انتشار ظاهرة الجريمة المنظمة، والتي تنتوع فيها أركان الجريمة وتتجاوز آثارها إقليم أكثر من دولة، حيث لا توجد هناك دولة معنية مباشرة بأمر الجريمة، وذلك مثل جرائم الإرهاب، والاتجار فى المواد المخدرة، والاتجار بالبشر، وغسل الأموال، والجرائم الإلكترونية.

وهناك مبرر آخر للأخذ بمبدأ الاختصاص الجنائى العالمى، يتمثل فى تقدم وسائل المواصلات والاتصالات فى العصر الحديث على نحو جعل انتقال الأشخاص من دولة لأخرى أمراً ميسوراً، وهو ما ساعد المجرمين على التخفى والفرار^(٤).

وهذا المبدأ ينبع من فكرة التعاون الدولى فى مكافحة الإجرام، والرغبة فى الحيلولة دون إفلات المجرمين من العقاب بعد أن ازدادت مظاهر الإجرام الدولى، وتخطى الإجرام حدود الدولة الواحدة فظهر ما يسمى بالجرائم المنظمة العابرة للقارات، لذلك اتجهت الأفكار إلى تجاوز مبدأ إقليمية القانون الجنائى إلى جعل الاختصاص لكل دولة فى انطباق قانونها على الجريمة أياً كان مكان ارتكابها أو شخص مرتكبها وجنسيته، متى ضبط مرتكبها فوق إقليم الدولة^(٥).

(١) د/ طارق سرور، المرجع السابق، ص ٢٥.

(٢) د/ سليمان عبد المنعم، دروس فى القانون الجنائى الدولى، دار الجامعة الجديدة، ٢٠٠٠، ص ٧٦.

(٣) د/ طارق سرور، المرجع السابق، ص ٢٦.

(٤) د/ سليمان عبد المنعم، النظرية العامة لقانون العقوبات، المرجع السابق، ص ١٣٨ وما بعدها.

(٥) د/ عبد الرؤوف مهدى، المرجع السابق، ص ١٥٣ وما بعدها؛ د/ أحمد شوقى أبو خطوة، المرجع السابق، ص ١٢٦.

وهذا المبدأ تمليه اعتبارات التعاون بين الدول من أجل مكافحة الجريمة ومنع إفلات المجرمين من العقاب.

٣- شروط الاختصاص الجنائي العالمي فى قانون مكافحة جرائم تقنية المعلومات:

ورد النص على مبدأ الاختصاص الجنائي العالمي فى المادة الثالثة من قانون مكافحة جرائم تقنية المعلومات التى قررت بأنه " مع عدم الإخلال بأحكام الباب الأول من الكتاب الأول من قانون العقوبات، تسري أحكام هذا القانون على كل من ارتكب خارج جمهورية مصر العربية من غير المصريين جريمة من الجرائم المنصوص عليها فى هذا القانون، متى كان الفعل معاقباً عليه فى الدولة التى وقع فيها تحت أى وصف قانوني، وذلك فى أى من الأحوال الآتية: ١- ... ٦- إذا وُجد مرتكب الجريمة فى جمهورية مصر العربية، بعد ارتكابها ولم يتم تسليمه."

وباستقراء نص المادة الثالثة - سالفه البيان - يتبين أنه يشترط لانعقاد الاختصاص الجنائي العالمي للقضاء المصرى - بنظر الجرائم الواردة فى قانون مكافحة جرائم تقنية المعلومات - توافر شرطين:

الشرط الأول: وجود مرتكب الجريمة فى مصر.

يشترط فضلاً عن أن يكون مرتكب الجريمة، أجنبياً أو عديم الجنسية، وذلك حتى ينعقد الاختصاص الجنائي للقضاء المصرى، أن يكون مرتكب تلك الجريمة موجوداً فى مصر.

ولا شك أن وجود المتهم على أرض مصر التى تمارس الاختصاص الجنائي العالمي من شأنه أن يولد ارتباطاً بينها وبين المتهم، الأمر الذى يبرر ويسهل معه من الناحية العملية ممارسة الاختصاص الجنائي العالمي بشأن جرائم تقنية المعلومات التى ترتكب فى الخارج^(١).

(١) Donnedieu de Vabres (Henri), Pour quels délits convient-il d'admettre la compétence universelle? R.I.D.P 1932, p 315.

من التشريعات التى نصت على هذا الشرط لانعقاد الاختصاص الجنائي العالمي لقضاها الوطنى: قانون الإجراءات الجنائية الفرنسى (المادة ١٠-٦٨٩) وقانون التحقيق الجنائي البلجيكي (المادة ١٢). د/ طارق سرور، المرجع السابق، ص ٢٧٢. حيث يرى سيادته أن شرط وجود المتهم على أرض الدولة لممارسة الاختصاص الجنائي العالمي، يمكن اعتباره شرطاً مفترضاً لتطبيق الالتزام التخييري بين التسليم أو المحاكمة.

ويفسر وجود المتهم في مصر - طبقاً للمادة (٣) من قانون مكافحة جرائم تقنية المعلومات - تفسيراً واسعاً، حيث يرمى إلى الاكتفاء بوجود المتهم بإقليم الدولة - مصر - ولو كان بصفة عابرة، فلا يشترط توافر رابطة معينة تربط المتهم بالدولة (مصر) ^(١).

وإذا وُجد المتهم - الأجنبي أو عديم الجنسية - بإقليم الدولة، فلا عبء بوسيلة دخوله إقليم الدولة، فيستوى أن يكون دخوله بطريقة مشروعة أو غير مشروعة، ولا أهمية بعد ذلك لأن يكون استمرار وجود المتهم في إقليم الدولة مخالفاً لقانونها الداخلي بعد أن كانت إقامته قانونية قبل ذلك. ولا يؤثر هروب المتهم بعد ذلك في انعقاد الاختصاص للقضاء الوطني بمحاكمة المتهم ^(٢)، ذلك أن هروبه لا يؤثر في استمرار المحاكمة ^(٣).

(١) يقصد بالتفسير الضيق لوجود المتهم بإقليم الدولة، الإقامة في إقليم الدولة لفترة بسيطة على الأقل بعد ارتكاب الجريمة، وفي هذا الإطار فقد اشترط القضاء الألماني لممارسة الاختصاص الجنائي العالمي أن يكون المتهم الذي قبض عليه مقيماً باختياريه في ألمانيا منذ عدة شهور ويتخذها مركزاً لحياته. د/ طارق سرور، المرجع السابق، ص ٢٧٣.

ولم يأخذ القضاء الفرنسي بالمفهوم الضيق لوجود المتهم بإقليم الدولة، كما هو الشأن في القضاء الألماني الذي يشترط توافر ارتباط معين بين المتهم والدولة لمدة معينة، كأن يتخذها مركزاً لحياته أو نشاطه. المرجع السابق، ص ٢٧٥.

(٢) وفقاً للمادة الثانية من القانون رقم ٨٩ لسنة ١٩٦٠ في شأن دخول وإقامة الأجانب بأراضي الجمهورية والخروج منها، لا يجوز دخول أراضي الجمهورية إلا لمن يحصل على جواز سفر سارى المفعول صادر من سلطات بلده المختصة أو أية سلطة أخرى معترف بها أو وزارة الداخلية أو لمن يحمل وثيقة تقوم مقام الجواز وتكون صادرة من إحدى السلطات المذكورة، ويشترط فيها أن تحول حاملها العودة إلى البلد الصادر من سلطاته، ويجب أن يكون الجواز أو الوثيقة مؤشراً عليه من وزارة الداخلية أو من إحدى السلطات السياسية أو القنصلية لجمهورية مصر العربية أو أي هيئة أخرى تندها. ووفقاً للمادة الرابعة من ذات القانون، لا يجوز دخول أراضي الجمهورية أو الخروج منها إلا من الأماكن التي يحددها وزير الداخلية بقرار يصدر منه وبإذن من الموظف المختص ويكون ذلك بالتأشير على جواز السفر أو الوثيقة التي تقوم مقامه. ويعاقب على مخالفة هذا النص أو القرارات الصادرة تنفيذاً له بالحبس مدة لا تزيد على ثلاثة أشهر وبغرامة لا تقل عن خمسين جنياً مصرياً ولا تزيد على مائتي جنياً أو بإحدى هاتين العقوبتين، وتكون العقوبة الحبس مدة لا تقل عن سنتين ولا تزيد عن خمس سنوات وبغرامة لا تقل عن مائتي جنياً ولا تزيد عن خمسمائة جنياً مصرياً إذا كان المخالف أو الأجنبي من رعايا دولة في حالة حرب مع مصر أو في حالة قطع علاقات سياسية معها، ومع عدم الإخلال بالمحاكمة الجنائية أو تنفيذ العقوبة يجوز إبعاد الأجنبي عن البلاد. د/ عصام الدين القصبى، د/ رشا على الدين، القانون الدولي الخاص، بدون دار نشر، ٢٠٠٩، ص ٥٤٢.

(٣) Bassiouni (Cherif), International Extradition, fourth edition, Oceana Publications, 2002, p8.

نقلاً عن د/ طارق سرور، المرجع السابق، ص ٢٧٥.

الشرط الثاني: وجود الجانى فى مصر وعدم تسليمه.

يشترط لتطبيق مبدأ الاختصاص الجنائى العالمى بحق فاعل جريمة من الجرائم الإلكترونية المرتكبة بالخارج، وجود الجانى فى مصر بعد ارتكاب الجريمة وعدم تسليمه، بأن يتم إلقاء القبض عليه فى مصر أو أن يكون مقيماً فيها بعد ارتكاب الجريمة.

ويستوى وجود الجانى بالإقليم البرى أو المائى أو الجوى، فإذا لم يتم القبض على الجانى فى مصر فلا تجوز محاكمته غيابياً، أما إذا قبض عليه وتم البدء فى اتخاذ إجراءات الاستدلال أو التحقيق أو المحاكمة ثم هرب الجانى فيجوز محاكمته غيابياً. وقد أكدت على هذا الشرط المادة ٦/٣ من قانون مكافحة جرائم تقنية المعلومات بأن قررت بأنه " إذا وُجد مرتكب الجريمة فى جمهورية مصر العربية، بعد ارتكابها ...".

ويكمل هذا الشرط ضرورة ألا يكون الجانى قد طُلب تسليمه - أو قُبِل أو تم - من الدولة التى وقعت الجريمة على أراضيها أو الدولة التى يحمل الجانى جنسيتها أو قُدم طلب من الدولة صاحبة الاختصاص الجنائى العالمى وقُبِل. وقد اشترطت ذلك الفقرة السادسة من المادة (٣) - سالفه البيان - بقولها " ولم يتم تسليمه".

٤- الاختصاص الجنائى العالمى فى قانون مكافحة جرائم تقنية المعلومات اختصاص مقيد:

إذا كانت الدول قد اتفقت على وضع حد لإفلات مرتكبي الجرائم الدولية، وذلك عن طريق ممارستها الولاية القضائية الجنائية، على مرتكبي هذه الجرائم الدولية. إلا أنه قد لا يشترط التشريع الوطنى شروطاً خاصة لانعقاد ولاية قضائه الوطنى، بمعنى ألا يتطلب القانون الوطنى توافر أية صلة أو ضابط يربط الجريمة أو مرتكبها أو المجنى عليه بالدولة لانعقاد اختصاص سلطاتها بملاحقة ومحاكمة ومعاقبة مرتكبي هذه الجرائم. وفى هذه الحالة يكون الاختصاص الجنائى للقضاء الوطنى اختصاصاً مطلقاً.

ومع ذلك فقد يشترط القانون الوطنى شروطاً لإعمال الاختصاص الجنائى العالمى، وهذه الشروط يتطلبها التشريع الوطنى لانعقاد ولايته القضائية بنظر الجرائم الدولية التى وقعت خارج إقليم الدولة، وفى هذه الحالة يكون انعقاد الاختصاص القضائى مشروطاً بتوافر شرط أو ضابط معين لانعقاد الاختصاص، وهو ما يسمى "بالاختصاص الجنائى العالمى المقيد". وفيه يُتطلب توافر ضابط أو شرط لانعقاد الاختصاص للقضاء

الوطني، كضبط مرتكب الجريمة في إقليم الدولة، وذلك حتى ينعقد الاختصاص لمحاكمها وسلطاتها الوطنية.

فالاختصاص الجنائي العالمي المطلق هو الاختصاص الذي يجوز ممارسته دون اشتراط أى ضابط يربط المتهم بالدولة، أو أى شرط لانعقاد الاختصاص للقضاء الوطني بنظر الجرائم الدولية. فالاختصاص الجنائي الدولي يكون مطلقاً إذا نص المشرع على انعقاد الولاية القضائية للقضاء الجنائي الوطني بنظر الجرائم الدولية والتي ترتكب خارج إقليم الدولة ولو لم يوجد المتهم بإقليم الدولة.

أما الاختصاص الجنائي العالمي المقيد فهو الاختصاص المشروط بشروط معينة وضوابط محددة لانعقاد الاختصاص الجنائي العالمي للقضاء الوطني تجمع بين المتهم والدولة التي ينعقد الاختصاص لقضائها، أهمها وجود مرتكب الجريمة في إقليم الدولة^(١).

وعلى ذلك، فإن الاختصاص الجنائي العالمي في قانون مكافحة جرائم تقنية المعلومات، يعد اختصاصاً مقيداً، ذلك أن المادة (٣) من هذا القانون، اشترطت لسريان أحكام هذا القانون على مرتكب جريمة من الجرائم المنصوص عليها فيه، خارج مصر في الحالة السادسة من تلك المادة - والخاصة بالاختصاص الجنائي العالمي - أن يكون مرتكب الجريمة - الأجنبي - موجوداً في مصر ولم يتم تسليمه.

(١) د/ طارق سرور، المرجع السابق، ص ٢٤٧ وما بعدها.

المطلب الخامس

شروط اختصاص السلطات المصرية بجرائم تقنية المعلومات المرتكبة فى الخارج

فضلاً عن الشروط الخاصة بكل حالة من الحالات الستة الواردة فى المادة (٣) من قانون مكافحة جرائم تقنية المعلومات، فلكى ينعقد الاختصاص للسلطات المصرية بمباشرة إجراءات الاستدلال والتحقيق والمحاكمة عن الجرائم الإلكترونية - الواردة فى هذا القانون - التى تقع بالخارج، لا بد من توافر الشروط الثلاثة الآتية:

الشرط الأول: مراعاة حكم المادة الرابعة من قانون العقوبات.

الشرط الثانى: ازدواج التجريم.

الشرط الثالث: ارتكاب جريمة الإلكترونية من غير المصريين.

الشرط الأول: مراعاة حكم المادة الرابعة من قانون العقوبات.

أشارت الفقرة الثانية من المادة الرابعة من قانون العقوبات إلى هذا القيد فى تحريك الدعوى الجنائية عن الجرائم المرتكبة فى الخارج بقولها " لا تقام الدعوى العمومية على مرتكب جريمة أو فعل فى الخارج إلا من النيابة العمومية، ولا تجوز إقامتها على من يثبت أن المحاكم الأجنبية برأته مما أسند إليه أو أنها حكمت عليه نهائياً واستوفى عقوبته".

فلا يجوز للنيابة العامة إقامة الدعوى الجنائية ضد مرتكب جريمة من الجرائم - المنصوص عليها فى قانون مكافحة جرائم تقنية المعلومات - المرتكبة فى الخارج إذا حوكم الجانى أمام المحاكم الأجنبية، وقضت ببراءته أو حكمت عليه نهائياً واستوفى عقوبته.

وعلى ذلك حتى يمتنع على النيابة العامة تحريك الدعوى الجنائية على مرتكب جريمة من هذه الجرائم - سألقة البيان - التى وقعت فى الخارج، لا بد من توافر الشرطين التاليين:

١- محاكمة المتهم في الخارج أمام محكمة أجنبية:

فإذا صدر قرار بحفظ التحقيق في الدولة الأجنبية عن جريمة من هذه الجرائم فلا يمنع من ذلك محاكمة الجاني في مصر، وكذلك الحال إذا انقضت الدعوى الجنائية بالتقادم، أو سقوط العقوبة بمضى المدة، أو صدور عفو شامل أو عفو عن العقوبة لمصلحة المتهم، فهذه الأسباب كافة لا تحول دون تحريك الدعوى الجنائية.

وقد أكدت ذلك محكمة النقض حيث قضت بأنه " لما كان الشارع قد حصر في النص المتقدم (المادة الرابعة عقوبات) القيود المانعة من إعادة تحريك الدعوى ضد المتهم في حالتي البراءة أو الإدانة المتبوعة بتنفيذ العقوبة، فإن ذلك يعنى استبعاد ما عداهما من الأسباب الأخرى كتقادم الدعوى أو العقوبة طبقاً للقانون الأجنبي أو صدور عفو شامل أو عفو عن العقوبة لمصلحة المتهم أو حفظ سلطات التحقيق للدعوى، فهذه الأسباب كافة لا تحول دون تحريك الدعوى الجنائية في مصر"^(١).

٢- صدور حكم نهائي في الدعوى الجنائية من المحاكم الأجنبية:

سواء بالبراءة أو بالإدانة واستيفاء العقوبة كاملة، ويستوى أن يصدر الحكم النهائي بالبراءة، أو بالإدانة مع تنفيذ العقوبة كاملة، ففي الحالتين يتمتع إقامة الدعوى الجنائية ذلك أنه لا يجوز محاكمة الشخص عن فعل واحد مرتين، وهذا أمر تمليه اعتبارات العدالة. والعبارة في نهائية الحكم بقانون البلد الذي صدر فيه^(٢).

وعلى ذلك فهناك حالتين لا يجوز فيهما تحريك الدعوى الجنائية ضد مرتكب جريمة من الجرائم الإلكترونية - المنصوص عليها في قانون مكافحة جرائم تقنية المعلومات - وقعت في الخارج وهما: حالة صدور حكم من المحاكم الأجنبية بالبراءة، وحالة صدور حكم بالإدانة واستيفاء العقوبة.

الحالة الأولى: صدور حكم بالبراءة.

تمتنع إعادة محاكمة مرتكب أي من هذه الجرائم - سالفه البيان - في الخارج في حالة صدور حكم نهائي بالبراءة أيًا كانت الأسباب الموضوعية للبراءة، كعدم ثبوت الواقعة أو عدم نسبتها للمتهم، أو عدم صحة الواقعة، أو عدم كفاية الأدلة.

(١) نقض جنائي، ٦ فبراير ٢٠٠٥، مجموعة أحكام محكمة النقض، س ٥٦ ص ١٠٨ رقم ١٣.

(٢) د/ محمود مصطفى، شرح قانون العقوبات، القسم العام، ١٩٨٣، ص ١٣٥.

الحالة الثانية: صدور حكم بالإدانة واستيفاء العقوبة كاملة.

فصدور حكم نهائى بالإدانة من المحكمة الأجنبية، وتنفيذ العقوبة المقضى بها، يمنع من إقامة الدعوى الجنائية فى مصر عن جريمة من هذه الجرائم التى وقعت بالخارج، أياً كانت العقوبة المقضى بها على الجانى، وسواء أكانت عقوبة أم تدبيراً احترازياً. ولا يشترط بعد ذلك أن تكون العقوبة الصادرة من المحكمة الأجنبية من نوع العقوبات المعروفة فى القانون المصرى، فضلاً عن أنه لا يشترط أن تكون أشد أم أخف من العقوبة المقررة للجريمة فى القانون المصرى لمكافحة جرائم تقنية المعلومات، ولا يشترط أخيراً أن يكون هناك اتحاد فى الوصف القانونى للجريمة فى كلا التشريعين الأجنبى والمصرى^(١).

وكل ما تشترطه المادة الرابعة من قانون العقوبات المصرى هو أن يقوم الجانى بتنفيذ الحكم الصادر من المحكمة الأجنبية، عن طريق استيفاء العقوبة المقضى بها استيفاءً كاملاً.

ذلك أنه طالما أصبح الحكم الصادر من المحكمة الأجنبية نهائياً^(٢)، وقام المحكوم عليه فى الجريمة بتنفيذ العقوبة المقضى بها تنفيذاً كاملاً، فإن ذلك الحكم يكتسب حجية تمنع من إعادة المحاكمة، حتى ولو كان وصف الجريمة فى القانون الأجنبى أقل خطورة من وصفها فى قانون مكافحة جرائم تقنية المعلومات المصرى.

أما إذا لم تنفذ العقوبة كلها أو جزء منها، فيجوز إعادة محاكمة مرتكب الجريمة التى وقعت بالخارج أمام القضاء المصرى، وفى حالة صدور حكم بالإدانة يتم احتساب المدة التى قضاها فى الحجز أو الحبس الاحتياطى أو تنفيذ العقوبة فى الخارج.

الشرط الثانى: ازدواج التجريم.

إن أهم مبدأ ساد القانون الجنائى، هو مبدأ الشرعية الجنائية، ويعنى هذا المبدأ أنه "لا جريمة ولا عقوبة إلا بنص قانونى". أى أن القانون المكتوب وحده هو الذى يحدد الأفعال المعتبرة جرائم، وهو وحده الذى يحدد العقوبات المقررة على ارتكابها.

(١) د/ عبد الرؤوف مهدى، شرح القواعد العامة لقانون العقوبات، المرجع السابق، ص ١٦١.

(٢) استعمل المشرع فى المادة الرابعة من قانون العقوبات عبارة " حكمت عليه نهائياً " للدلالة على الحكم النهائى، والصحيح أنه الحكم البات. د/ عبد الرؤوف مهدى، شرح القواعد العامة لقانون العقوبات، المرجع السابق، ص ١٥٨؛ د/ محمود نجيب حسنى، قوة الحكم الجنائى فى إنهاء الدعوى الجنائية، بدون دار نشر، ١٩٧٧، ص ٧٨.

ويتمتع مبدأ الشرعية الجنائية بالطابع الدستوري، حيث قررت المادة ٩٥ من الدستور بأنه " لا جريمة ولا عقوبة إلا بناء على قانون ولا توقع عقوبة إلا بحكم قضائي، ولا عقاب على الأفعال اللاحقة لتاريخ نفاذ القانون " .

وهذا الطابع الدستوري - لمبدأ الشرعية الجنائية - تتمثل قيمته في أنه يُفرض على المشرع نفسه، فلا يستطيع أن يخالف مبدأ الشرعية الجنائية بأن يصدر تشريعاً يمنح فيه القضاة سلطة تجريم الأفعال أو سلطة تحديد اختصاص المحاكم، وإذا حدث وصدر تشريع لا يحترم الحدود الدستورية، فإن للقاضي أن يمتنع عن تطبيقه لمخالفته للدستور .

وبالنظر إلى القانون رقم ١٧٥ لسنة ٢٠١٨ في شأن مكافحة جرائم تقنية المعلومات، نجد أنه قد احترم مبدأ الشرعية الجنائية حين اشترط ازدواج التجريم في كل من القانونين المصري والأجنبي، وذلك بأن اشترط لتطبيق أحكام هذا القانون على مرتكب جريمة من الجرائم المنصوص عليها فيه خارج جمهورية مصر العربية - من غير المصريين - أن يكون الفعل معاقباً عليه في الدولة التي وقع فيها تحت أي وصف قانوني .

فقد تطلب المشرع - في المادة الثالثة - أن يكون الفعل المرتكب في الخارج معاقباً عليه طبقاً لقانون الدولة التي ارتكب فيها، أيأ كانت درجة جسامته هذا الفعل وأياً كان نوع العقوبة المقررة له .

فإذا كان القانون الأجنبي لا يعاقب على الفعل تحت أي وصف فلا يسرى القانون المصري لمكافحة جرائم تقنية المعلومات ولو كان الفعل يعد جريمة وفقاً لأحكامه، وذلك لأن الشخص يتقيد أثناء وجوده في الخارج بقوانين الدولة التي يوجد في إقليمها، فلا يجوز معاقبته عن فعل لم يحظره هذا القانون .

الشرط الثالث: ارتكاب الجريمة من غير المصريين .

اشترطت المادة (٣) من قانون مكافحة جرائم تقنية المعلومات - لسريان أحكام هذا القانون على كل من ارتكب جريمة من الجرائم المنصوص عليها فيه خارج مصر - أن يكون مرتكب الجريمة من غير المصريين . وهو قد يكون أجنبياً أو عديم الجنسية .

والأجنبي، هو كل شخص لا يحمل جنسية جمهورية مصر العربية، سواء أكان يحمل جنسية دولة أو دول أخرى أم كان لا يحمل أية جنسية على الإطلاق^(١). فالمعيار المميز "للأجنبي" عن "المواطن" هو معيار الجنسية، أما معيار الموطن أو محل الإقامة الدائمة فلا يفيد في التمييز بينهما. فمن لا يحمل جنسية الدولة يظل أجنبياً عنها، مهما طال مدة إقامته على إقليمها^(٢).

وعديم الجنسية، هو الشخص الذى تتخلى عنه قوانين الجنسية فى كافة دول العالم، فلا تمنحه أية دولة الصفة الوطنية. فانعدام الجنسية هو عبارة عن الحالة التى تنكر فيها كافة القوانين فى كل الدول تبعية الفرد لها، مما يؤدى إلى اعتباره عديم الجنسية^(٣).

فإذا ارتكب المصرى جريمة من الجرائم المنصوص عليها فى قانون مكافحة جرائم تقنية المعلومات، خارج مصر فإن هذا القانون يسرى على هذا الشخص تطبيقاً لمبدأ الشخصية الإيجابية، وليس إعمالاً لمبدأ الاختصاص الجنائى العالمى، وذلك متى توافرت شروط تطبيق المبدأ الأول.

(١) د/ هشام على صادق، موجز القانون الدولى الخاص، الدار الجامعية، ١٩٨٦، ص ٥ وما بعدها.

(٢) د/ محمد السيد عرفة، الجنسية ومركز الأجنبي، دار الفكر والقانون بالمنصورة، ٢٠١٢، ص ٢٨١.

(٣) يكون عديم الجنسية فى وضع شاذ، فلا هو مواطن ولا هو أجنبى يتمتع بحماية دولة معينة، وإنما هو أجنبى عن كل الدول، فهو أجنبى من نوع خاص. ويشبه أحد الفقهاء عديم الجنسية بالسفينة التى تجرى فى أعالي البحار دون علم، ومن ثم دون حماية. د/ محمد السيد عرفة، المرجع السابق، ص ١٣٧.

الخاتمة

انتهينا من خلال عرضنا لموضوع المواجهة الجنائية للجرائم الإلكترونية - فى ضوء قانون مكافحة جرائم تقنية المعلومات - إلى مجموعة من النتائج والتوصيات.

أولاً: النتائج.

١- الجريمة الإلكترونية هى كل فعل أو امتناع عن فعل من خلال الوسائل الإلكترونية، يهدف إلى الاعتداء على أية مصلحة مشروعة سواء كانت مادية أو معنوية.

٢- للجريمة الإلكترونية مجموعة من الخصائص تتفرد بها عن الجرائم التقليدية، فهذه الجرائم تتطلب وجود جهاز إلكترونى ومعرفة كيفية استخدامه، كما أن هذه الجريمة لا حدود لها، فضلاً عن أنها جريمة صعبة الإثبات والاكتشاف.

٣- أن الاستعانة بالخبراء فى الجرائم الإلكترونية، أمر لا بد منه فى جميع مراحل الدعوى الجنائية وجمع الاستدلالات والتحقيق والمحاكمة.

٤- أصدر المشرع المصرى القانون رقم ١٧٥ لسنة ٢٠١٨ - فى شأن مكافحة جرائم تقنية المعلومات - استجابة للتطور التكنولوجى السريع والمتنامى فى مجال نظم تقنية المعلومات، وذلك بهدف مواجهة الاستخدام غيرالمشروع لتقنية المعلومات، فضلاً عن حماية حرمة الحياة الخاصة.

ثانياً: التوصيات.

١- ضرورة إعادة النظر فى النظم الإجرائية المتعلقة بإجراءات التحرى والتحقيق فى الجرائم الإلكترونية، بما يتناسب مع الطبيعة الذاتية لتلك الجرائم.

٢- تفعيل التعاون القضائى الدولى فى مكافحة الجرائم الإلكترونية ليشمل تيسير تبادل المعلومات والبحث والتحرى والاستدلال بين أجهزة الضبط القضائى المختصة فى مختلف دول العالم، والتوسع فى مجال المساعدة القانونية والقضائية المتبادلة وكذا الإنابة القضائية وتسليم المجرمين.

٣- ضرورة الانضمام إلى الاتفاقيات الدولية المعنية بمكافحة الجرائم الإلكترونية، وأهمها اتفاقية بودابست الخاصة بمكافحة الجرائم المعلوماتية، والاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

٤- أهمية عقد الدورات التدريبية وورش العمل للقائمين على إنفاذ التشريعات الخاصة بمكافحة الجرائم الإلكترونية، من السادة القضاة وأعضاء النيابة العامة ومأموري الضبط القضائي، وذلك لبناء وزيادة قدراتهم على التعامل مع كافة الدعاوى المتعلقة بالجرائم الإلكترونية وكيفية التحقيق في تلك الجرائم وإثباتها، وصولاً إلى مواجهة فاعلة في هذا الشأن.