وسائل مكافحة الجرائم الالكترونية في الكويت

تعاني مجتمعاتنا العربية في العصر الحالي من آفة خطيرة تهدد أمن وأمان الفرد والمجتمع على على حد سواء، وتتمثل تلك الآفة في الجريمة الإلكترونية بأنواعها وصورها المختلفة، وتنبع خطورة تلك الجريمة في كونها لا تتطلب انتقال الجاني إلى مكان وجود المجني عليه، بل يمكن للجاني أن يرتكب جريمته بكل سهولة خلال وجود المجني عليه في بيته ووسط عائلته، حيث لا يتطلب الأمر سوى ضغطة زر على لوحة مفاتيح الحاسب الآلي أو الهاتف الذكي ليرتكبها، وهو ما يجعلها من الجرائم التي يسهل ارتكابها، بما يرفع من معدلات خطورتها خاصة في ظل التقدم التطور الذي يتزايد يوماً بعد يوم في مجال تقنية المعلومات.

لذلك فإن المجتمع بكافة فئاته يتكاتف مع الحكومة لمواجهة مثل تلك الجرائم الخطيرة على كافة الأصعدة، لاسيما وأن المواجهة التشريعية لا تكفي وحدها لمكافحة الجرائم الإلكترونية، بل يلزم أن يتحقق معها مستوى عالي من الوعي بين أفراد المجتمع، وذلك حتى تتم مواجهتها على محورين، محور سابق على وقوع الجريمة للوقاية من ارتكابها، ومحور لاحق على ارتكاب الجريمة لمواجهة آثارها.

لذلك فسوف نتعرض في هذا المقال الى وسائل مكافحة الجرائم الالكترونية بأنواعها المختلفة، حيث سنوضح وسائل المكافحة القانونية، والمتمثلة في العقوبات التي قررها المشرع الكويتي في قانون مكافحة جرائم تقنية المعلومات رقم 63 لسنة 2015، ووسائل المكافحة غير القانونية والمتمثلة في الجهود المجتمعية والمؤسسية المختلفة التي تبذل من قبل الأفراد والمؤسسات الحكومية وغير الحكومية في هذا الشأن.

أولاً: ماهية الجريمة الإلكترونية

قبل أن نتناول وسائل مكافحة الجرائم الإلكترونية يلزمنا بداية أن نتعرف على ماهية الجريمة الإلكترونية، لاسيما وأنها المحور الأساسي لهذا المقال، كما أنها جريمة حديثة العهد في الظهور، وبالتالي قد لا يكون لدى البعض العلم الكافي بماهيتها.

اختلف الفقه حول تعريف هذه الطائفة من الجرائم إلى أكثر من اتجاه، وكان منبع هذا الاختلاف هو اختلاف المنظور الذي اتخذه كل اتجاه منهم في تعريفه للجريمة الإلكترونية، حيث عرفها البعض من منظور صفات الجاني فيها بأنها الجرائم التي يقوم الجاني فيها قدراته ومعارفه الخاصة بتقنية المعلومات والحاسب الآلي والفضاء الإلكتروني، بينما عرفها اتجاه آخر من منظور أداة الجريمة بأنها فعل غير مشروع يرتكبه الجاني باستخدام الحاسب الآلي كأداة أساسية للجريمة.

وقد جاء المشرع الكويتي حاسماً لهذا الاختلاف، حيث تعرض بالتعريف للجريمة الإلكترونية تحت مسمى الجريمة المعلوماتية، وذلك بنص المادة الأولى من القانون رقم 63 لسنة 2015 في شأن جرائم تقنية المعلومات، حيث عرفها بأنها "كل فعل يرتكب من خلال استخدام الحاسب الآلي أو الشبكة المعلوماتية أو غير ذلك من وسائل تقنية المعلومات بالمخالفة لأحكام هذا القانون".

ثانياً: الوسائل التشريعية لمكافحة الجريمة الإلكترونية

تتجسد الوسيلة التشريعية التي قررها المشرع الكويتي لمكافحة الجرائم الإلكترونية في القانون رقم 63 لسنة 2015 في شأن مكافحة جرائم تقنية المعلومات، والذي من خلاله نص على مجموعة من الأدوات الأساسية التي استخدمها لمواجهة هذه الطائفة من الجرائم، ونقصد بتلك الأدوات العقوبات المتنوعة التي استخدمها المشرع لمعاقبة مرتكبي الجرائم الإلكترونية التي وردت بنصوص التجريم، حيث قرر المشرع لكل صورة من صور الجريمة الإلكترونية عقوبة أو أكثر تتناسب مع خطورتها، وقد تنوعت تلك العقوبات بين عقوبات أصلية وعقوبات تبعية، ويمكننا أن نوجز تلك العقوبات على النحو التالي:

(1) العقوبات الأصلية: وتتمثل هذه العقوبات في نوعين من العقوبات:

- **عقوبة سالبة للحرية:** وتتمثل في عقوبة الحبس، وهذه العقوبة تتباين في مدتها بحسب الجريمة التي ارتكبها المجرم الذي توقع عليه تلك العقوبة.
- **عقوبة مالية:** وتتمثل في عقوبة الغرامة، والتي تختلف في قيمتها بحسب الجريمة التي ارتكبها المجرم الذي يتم إلزامه بتلك العقوبة.

مع ملاحظة أن المشرع قد منح قاضي الموضوع الذي ينظر الدعوى سلطة تقديرية في تقدير جسامة الجريمة، بحيث يجوز له توقيع إحدى هاتين العقوبتين (حبس أو غرامة) على المجرم، كما يجوز له أيضاً أن يوقع العقوبتين معاً.

(2) العقوبات التكميلية: يقصد بالعقوبات التكميلية العقوبات التي توقع بشكل إضافي للعقوبات الأصلية التي يتم الحكم بها على المتهم، بحيث لا يتم توقيع تلك العقوبات بشكل مستقل بل يتم الحكم بها لتكملة عقوبة أصلية، وقد قرر المشرع الكويتي نوعين من العقوبات التكميلية وتتمثل في:

- **عقوبة المصادرة:** ويقصد بالمصادرة كعقوبة تكميلية نزع ملكية أي أموال أو أدوات قام الجاني باستخدامها في ارتكاب جريمته، أو أن تكون تلك الأموال هي متحصلات قد نتجت عن ارتكابه تلك الجريمة، ويكون نزع ملكية هذه الأموال والأدوات لصالح خزينة الدولة دون مقابل، وفي الجرائم الإلكترونية تنصب عقوبة المصادرة كعقوبة تكميلية على كافة الأجهزة والبرامج أو غيرها من الوسائل المستخدمة في ارتكاب الجريمة الإلكترونية، بجانب مصادرة أي مبالغ مالية تم التحصل عليها كنتيجة لارتكاب هذه الجريمة.
- **عقوبة الغلق:** المقصود بالغلق كعقوبة تكميلية هو إغلاق المكان الذي تم استخدامه لارتكاب الجريمة بغض النظر عن نوع تلك الجريمة، وذلك منعاً لاستمرار استغلال هذا المكان في ارتكاب ذات المخالفة من جهة، ومن جهة أخرى استخدام تلك العقوبة كجزاء رادع لمرتكب الجريمة، وفي إطار قانون مكافحة جرائم تقنية المعلومات فإن عقوبة الغلق كعقوبة تكميلية تنصب على المحل أو الموقع الذي تم فيه ارتكاب أي جريمة من الجرائم الإلكترونية، إلا أن تلك العقوبة قد وردت بشكل جوازي تارة وبشكل وجوبي تارة أخرى:

- عقوبة الغلق الجوازية: تتمثل في الغلق المؤقت للمكان أو الموقع الذي تمت فيه الجريمة الإلكترونية لمدة لا تتجاوز سنة واحدة، ويكون توقيع تلك العقوبة مشروطاً

بأن تكون الجريمة الإلكترونية التي تم ارتكابها في هذا المكان أو الموقع الذي سيتم إغلاقه قد تمت بعلم مالك هذا المكان أو الموقع، ويكون توقيعها هو أمر جوازي لمحكمة الموضوع التي تنظر الدعوى، فلها أن تقضي بها أو لا تقضي بها حسب سلطة المحكمة التقديرية في تقدير جسامة الجريمة الإلكترونية المرتكبة.

- عقوبة الغلق الوجوبية: يتم توقيع تلك العقوبة التكميلية بشكل وجوبي، أي لا تخضع في توقيعها على السلطة التقديرية للمحكمة، بل يجب عليها أن تقضي بها مع العقوبة الأصلية، إلا أن ذلك مشروط بشرطين هامين، الأول هو أن يكون هذا المكان أو الموقع الذي سيتم الحكم بغلقه قد سبق وأن تم تكرار ارتكاب الجريمة الإلكترونية فيه من قبل، والثاني هو أن يكون ارتكاب تلك الجرائم الإلكترونية المتكررة بعلم مالك المكان أو الموقع، وبالتالي لا تُعد العقوبة وجوبية حتى وإن تكرر ارتكاب الجريمة الإلكترونية قي ذلات المكان أو الموقع متى كان ذلك قد تم بدون علم مالك المكان أو الموقع، فإذا توافر هذين الشرطين أصبح واجباً على المحكمة توقيع عقوبة الغلق مع العقوبة الأصلية.

ثالثاً: الوسائل غير القانونية (المجتمعية) لمكافحة الجريمة الإلكترونية

لا تقتصر وسائل مكافحة الجريمة الإلكترونية على الجهود التشريعية والقانونية فقط، بل توجد أيضاً وسائل أخرى غير قانونية – خارجة إطار القانون والتشريعات ذات العلاقة - يقوم بها المجتمع بأفراده ومؤسساته – حكومية وغير حكومية – بغرض مكافحة هذا النوع من الجرائم، وتعتمد تلك الوسائل على آلية نشر الوعي بين أفراد المجتمع بخطورة الجريمة الإلكترونية، وكيفية الوقاية من الوقوع ضحية لها، وما هو التصرف الأمثل الذي يجب اتخاذه في حالة الوقوع في براثن مجرم إلكتروني.

ويتم نشر هذا الوعي بين أفراد المجتمع من خلال عدة طرق يمكننا أن نذكر أهمها وأبرزها فيما يلي:

- عقد الندوات والمؤتمرات والفاعليات التي تتناول موضوع الجريمة الإلكترونية، والتي تتولى تنظيمها بالتعاون بين الجهات الحكومية المعنية ومؤسسات القطاع الخاص، ويتم خلالها استضافة بعض المتخصصين من رجال القانون للتوعية بمخاطر الجرائم الإلكترونية وكيفية الوقاية من الوقوع فيها سواء كجاني أو كمجني عليه، ومن أبرز الأمثلة على ذلك مؤتمر الكويت السابع لمكافحة الجرائم الإلكترونية، والذي تم فيه تناول أهم المستجدات التي طرأت على مجال الجرائم الإلكترونية، والطرق التي يمكن من خلالها التصدي لتلك الجرائم.
- إطلاق حملات التوعية عبر وسائل التواصل الاجتماعي المختلفة، والتي تستهدف رفع الوعي المجتمعي بمبادئ الأمان على شبكة الإنترنت، ومثال على تلك الحملات التوعوية الحملة التي قام بها بنك الكويت الوطني بالتعاون مع وزارة الداخلية ومؤسسة لوياك التطوعية، وحملة "لنكن على دراية" التي تم إطلاقها بالتعاون بين بنك الكويت المركزي واتحاد مصارف الكويت، وذلك للتوعية بمخاطر الجرائم الإلكترونية بوجه عام وجرائم الاحتيال المالي الإلكترونية بوجه خاص.

- إجراء الأبحاث والدراسات المتخصصة التي تستهدف التعريف بالجرائم الإلكترونية، والثغرات التي يمكن أن يتسلل منها الجاني لارتكاب مثل تلك الجرائم، وكيفية الوقاية من تلك الثغرات، والخروج ببعض التوصيات التي تساعد على ذلك، والتي يمكن أن نوجز أهمها فيما يلي:

- استخدام كلمات مرور قوية للحسابات الشخصية على المواقع الإلكترونية، يتم فيها المزج بين الحروف والأرقام والرموز، بحيث يصعب على الجناة اختراقها.
- عدم الضغط على أي لينكات أو روابط مجهولة يتم استقبالها على الأجهزة الإلكترونية أو الهواتف الذكية.
- استخدام برامج حماية وبرامج مضادة للفيروسات، على أن تكون تلك البرامج قوية وحديثة.
- الحفاظ على البيانات الشخصية وعدم إفشائها إلى أي شخص.
- اتباع نظام المصادقة الثنائية (2FA) لحماية الحساب الشخصي من الاختراق، حتى في الحالة التي تتم فيها سرقة كلمة المرور.
- الحث على ضرورة الإبلاغ عن حالات الابتزاز والتهديد الإلكتروني، لاسيما وأن هناك العديد من ضحايا تلك الجرائم الإلكترونية ينصاعون للمبتزين خوفاً على سمعتهم واعتبارهم في حال الإبلاغ عن تلك الجرائم.