مجلة جامعة الشارقة للعلوم القانونية

جامعة الشارقة
UNIVERSITY OF SHARJAH

مجلة جامعة الشارقة

مجلة علمية محكمة

للعلوم القانونية

المجلد 20، العدد 3
ربيع الأول 1443هـ / سبتمبر 2023م

الترقيم الدولي المعياري للدوريات 2616-6526

https//:doi.org/10.36394/jls.v20.i3.5

جريمة إتلاف محتويات البريد الإلكتروني في التشريع الإماراتي

مصعب عبدالله النقبي[1]

خالد محمد دقاني[2]

تاريخ الاستلام: 29-06-2021 **تاريخ القبول: 30-09-2021**

ملخص البحث:

يهدف البحث إلى تحديد مفهوم البريد الإلكتروني وطبيعته القانونية ومبررات حمايته، والوقوف على البنيان القانوني لجريمة إتلاف محتويات البريد الإلكتروني، وتوضيح مدى معالجة المشرع الإماراتي للجوانب الموضوعية المتعلقة بحماية البريد الإلكتروني من إتلاف محتوياته باستخدام التكنولوجيا الحديثة، وتتجلى أهمية البحث في أنّ موضوعه يسعى للإحاطة بالبنيان القانوني لجريمة إتلاف محتويات البريد الإلكتروني في التشريع الإماراتي، وذلك في ظل انتشار وتعدد وتنوع وسائل وتقنيات البيانات والمعلومات والاعتماد عليها من قبل الأفراد والجهات الحكومية في أعمالهم اليومية، وما ترتب على ذلك من اتساع وزيادة جرائم انتهاك الخصوصية والدخول غير المشروع إلى البريد الإلكتروني، والمخاطر التي تهدد البيانات والمعلومات الحكومية، وكذلك المراسلات البريدية السرية للمؤسسات المالية والتجارية والاقتصادية في الدولة، وقد توصل البحث إلى عدة نتائج أهمها أنّ المشرع الإماراتي لم يحدد على سبيل الحصر صور السلوك التي يتحقق بها الاعتداء على البريد الإلكتروني، ومن ثَمّ تتنوع صور السلوك التي تشكل اعتداء على البريد الإلكتروني، وتتمثل في فعل يرتكبه الجاني عمدياً، ويكون إتلاف محتويات البريد الإلكتروني من خلال ممارسة أي سلوك يترتب عليه هذا الإتلاف، وذلك كاستخدام شفرات ضارة ومدمرة وفيروسات تخريبية، وهي تنتقل من حاسب آلي إلى آخر، ومن بريد إلى آخر، أو أي سلوك آخر يحقق النتيجة ذاتها، طالما أن المشرع لم يحدد صور السلوك لوقوع جريمة إتلاف محتويات البريد مثلما لم يحدد لها نتيجة محددة.

الكلمات الدالة: البريد الإلكتروني، الإتلاف المعلوماتي، التشريع الإماراتي، المصلحة المحمية.

(1) كلية القانون - جامعة الشارقة (الشارقة - الإمارات العربية المتحدة)

malnaour@gmail.com

(2) كلية القانون - جامعة الشارقة (الشارقة - الإمارات العربية المتحدة)

المقدمة

مع تصاعد معدل ارتكاب الجرائم باستعمال وسائل تقنية المعلومات، ومنها استعمال البريد الإلكتروني في ارتكاب الجرائم ضد الأشخاص والأموال أو ضد المؤسسات الحكومية؛ إذ تمّ تسخير تقنية المعلومات في عمليات الإغلاق للبريد الإلكتروني من خلال الرسائل والملفات والتي قد تؤدي إلى إيقافه عن العمل أو تعطيله وإتلاف وسرقة محتوياته، وتم استخدامه في عمليات الاحتيال وارتكاب جرائم الاعتداء على حق الإنسان في سمعته وشرفه واعتباره، وأصبح الإنسان هدفًا من أهداف مجرمي تقنية المعلومات، وعليه كان لا بدّ أن تتوافق السياسة الجنائية لمشرع كل دولة وحق الفرد في سلامة بدنه واعتباره وشرفه وحريته وغيرها من الاعتبارات والمصالح المحمية بموجب القانون[1].

ولما كان من المسلم به أن الأنظمة المعلوماتية تبقى عرضة للاعتداءات، ولعل أهم هذه الاعتداءات التي تقع على البيانات الموجودة داخل الحاسب الآلي، فهي التي تمس بسلامتها وأمنها، وتعد جريمة (إتلاف محتويات البريد الإلكتروني) إحدى أبرز وأهم جرائم الاعتداء على الكيان المعنوي للحاسب الآلي، ناهيك على أنها لا تختلف عن بقية الجرائم الإلكترونية الواقعة على الأموال من حيث انطواؤها على اعتداء غير مشروع على حق الملكية، ومهما تنوعت أساليب الاعتداء، إلا أنها تنصب على فعل إتلاف البيانات المخزنة في البيئة الافتراضية[2].

وفي ظل الاعتداءات والانتهاكات الواقعة على الأشخاص والأموال التي قد ترتكب من خلال البريد الإلكتروني، فقد حظي بحماية جزائية من قبل المشرع الإماراتي سواء كان ذلك بواسطة الاختراق أو الإغلاق أو الإيقاف عن العمل أو إتلافه وسرقة ما يحتويه من معلومات؛ لأنّ ذلك يعد اعتداء على الخصوصية المعلوماتية التي كفلها الدستور الإماراتي[3]، كما جرم المشرع الإماراتي الدخول إلى البريد الإلكتروني والإطلاع على الرسائل الموجودة بداخله بغير إذن صاحبه، واعتبر ذلك اعتداءً على سرية المعلومات المكفولة بنصوص الدستور، وأقر المشرع حماية تلك المراسلات وضمن سريتها، حيث لا يجوز مراقبة أو انتهاك سرية البريد الإلكتروني أو الإطلاع على محتواه إلا في حدود

(1) محمود أحمد طه، التنصت والتلصص على سرية الاتصالات الشخصية بين التجريم والمشروعية، دار الفكر والقانون، المنصورة، مصر، 2018م، ص 9.

(2) عمار عباس الحسيني، جرائم الحاسوب والإنترنت، منشورات زين الحقوقية، بيروت، 2017م، ص 45-44.

(3) تنص المادة (31) من الدستور الاتحادي لدولة الإمارات العربية المتحدة على أنه: (حرية المراسلات البريدية والبرقية وغيرها من وسائل الاتصال وسريتها مكفولتان وفقا للقانون).

القانون[1]، كما جرم المشرع فعل الإتلاف لمحتويات البريد الإلكتروني في المرسوم بقانون اتحادي رقم (5) لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات وتعديلاته في المواد (2، 4، 5، 10)[2].

(1) تنص المادة (21) من قانون مكافحة جرائم تقنية المعلومات الإماراتي على أنه: (يعاقب بالحبس مدة لا تقل عن ستة أشهر والغرامة التي لا تقل عن مائة وخمسين ألف درهم ولا تجاوز خمسمائة ألف درهم أو بإحدى هاتين العقوبتين كل من استخدم شبكة معلوماتية، أو نظام معلومات إلكتروني، أو إحدى وسائل تقنية المعلومات، في الاعتداء على خصوصية شخص في غير الأحوال المصرح بها قانونا بإحدى الطرق التالية: -1 استراق السمع، أو اعتراض، أو تسجيل أو نقل أو بث أو إفشاء محادثات أو اتصالات أو مواد صوتية أو مرئية. -2 التقاط صور الغير أو إعداد صور إلكترونية أن نقلها أو كشفها أو نسخها أو الاحتفاظ بها. -3 نشر أخبار أو صور إلكترونية أو صور فوتوغرافية أو مشاهد أو تعليقات أو بيانات أو معلومات ولو كانت صحيحة وحقيقية. كما يعاقب بالحبس مدة لا تقل عن سنة واحدة والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تجاوز خمسمائة ألف درهم أو بإحدى هاتين العقوبتين، كلُّ من استخدم نظام معلومات إلكترونيًّا، أو إحدى وسائل تقنية المعلومات، لإجراء أي تعديل أو معالجة على تسجيل أو صورة أو مشهد، بقصد التشهير أو الإساءة إلى شخص آخر، أو الاعتداء على خصوصيته أو انتهاكها).

(2) تنص المادة (2) على أنه: (-1 يعاقب بالحبس والغرامة التي لا تقل عن مائة ألف درهم ولا تزيد على ثلاثمائة ألف درهم أو بإحدى هاتين العقوبتين كل من دخل موقعًا إلكترونيًّا أو نظام معلومات إلكترونيًّا أو شبكة معلومات، أو وسيلة تقنية معلومات، بدون تصريح أو بتجاوز حدود التصريح، أو بالبقاء فيه بصورة غير مشروعة. 2 - تكون العقوبة الحبس مدة لا تقل عن ستة أشهر والغرامة التي تقل عن مائة وخمسين ألف درهم ولا تجاوز سبعمائة وخمسين ألف درهم أو بإحدى هاتين العقوبتين إذا ترتب على أي فعل من الأفعال المنصوص عليها بالفقرة 1 من هذه المادة إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو نسخ أو نشر أو إعادة نشر أي بيانات أو معلومات. -3 تكون العقوبة الحبس مدة لا تقل عن سنة واحدة والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تجاوز مليون درهم أو بإحدى هاتين العقوبتين إذا كانت البيانات أو المعلومات محل الأفعال الواردة في الفقرة 2 من هذه المادة شخصية).

تنص المادة (4) على أنه: (يعاقب بالسجن المؤقت والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تجاوز مليون وخمسمائة ألف درهم كل من دخل بدون تصريح إلى موقع إلكتروني، أو نظام معلومات إلكتروني، أو شبكة معلوماتية، أو وسيلة تقنية معلومات، سواء كان الدخول، بقصد الحصول على بيانات حكومية، أو معلومات سرية خاصة بمنشأة مالية، أو تجارية، أو اقتصادية. وتكون العقوبة السجن مدة لا تقل عن خمس (5) سنوات والغرامة التي لا تقل عن خمسمائة ألف درهم ولا تتجاوز مليوني درهم، إذا تعرضت هذه البيانات أو المعلومات للإلغاء أو الحذف أو الإتلاف أو التدمير أو الإفشاء أو التغيير أو النسخ أو النشر أو إعادة النشر).

وتنص المادة (5) على أنه: (يعاقب بالحبس والغرامة التي لا تقل عن مائة ألف درهم ولا تجاوز ثلاثمائة ألف درهم أو بإحدى هاتين العقوبتين كل من دخل بغير تصريح موقعاً إلكترونياً بقصد تغيير تصاميمه أو إلغائه أو إتلافه أو تعديله أو شغل عنوانه). وتنص المادة (10) على أنه: "يعاقب بالسجن مدة لا تقل عن خمس سنوات والغرامة التي لا تقل عن خمسمائة ألف درهم ولا تجاوز ثلاثة ملايين درهم أو بإحدى هاتين العقوبتين كل من أدخل عمداً وبدون تصريح برنامجًا معلوماتيًا إلى الشبكة المعلوماتية أو نظامًا معلوماتيًّا إلكترونيًّا أو إحدى وسائل تقنية المعلومات، وأدى ذلك إلى إيقافها عن العمل أو تعطيلها أو تدمير أو مسح أو حذف أو إتلاف أو تغيير البرنامج أو النظام أو الموقع الإلكتروني أو البيانات أو المعلومات. وتكون العقوبة السجن والغرامة التي لا تجاوز خمسمائة ألف درهم أو إحدى هاتين العقوبتين إذا لم تتحقق النتيجة. وتكون العقوبة الحبس والغرامة أو إحدى هاتين العقوبتين عن أي فعل عمدي يقصد به إعراق البريد الإلكتروني بالرسائل وإيقافه عن العمل أو

أهمية البحث:

1. تجلت أهمية هذا البحث في أن هناك العديد من الأسباب التي دعت المشرع الإماراتي إلى سَنّ قوانين خاصة لمكافحة الجرائم التقنية، وهذه الأسباب تتمثل في التوسع باستخدام الإنترنت[1]، وخصوصاً وسيلة البريد الإلكتروني، ولما لهذا الموضوع من أهمية بالغة؛ إذ إنّ جميع القطاعات الحكومية والخاصة في دولة الإمارات تحولت إلى النظام الإلكتروني والذكي في إنجاز معاملاتها وخدماتها، وكان لا بدّ من حماية البريد الإلكتروني من أي اعتداءات غير مشروعة، كإغراقه بالملفات أو تعطيله أو بإيقافه عن العمل أو إتلاف محتوياته.

2. أن موضوعه يسعى للإحاطة بماهية جريمة إتلاف محتويات البريد الإلكتروني في التشريع الإماراتي، وذلك في ظل انتشار وتعدد وتنوع وسائل وتقنيات البيانات والمعلومات والاعتماد عليها من قبل الأفراد والجهات الحكومية في القيام بأعمالهم اليومية، وما ترتب على ذلك من اتساع وزيادة جرائم انتهاك الخصوصية والدخول غير المشروع إلى بيانات البريد الإلكتروني، والمخاطر التي تهدد بيانات الجهات الحكومية، وكذلك المراسلات البريدية السرية للمؤسسات المالية والتجارية والاقتصادية في الدولة[2].

تعطيله أو إتلاف محتوياته).

(1) وفقاً لتقرير (الحالة الرقمية في 2020) الصادر في مارس 2020 عن مؤسسة "هوتسوت" الكندية لرصد أوضاع الرقمنة ومستويات انتشار تقنيات الاتصال الحديثة بمختلف أدواتها في كافة دول العالم، تصدرت دولة الإمارات دول العالم في (6) مؤشرات هي: (انتشار الإنترنت بين إجمالي السكان، انتشار مواقع التواصل الاجتماعي بين إجمالي السكان، ونسبة الاشتراكات في خدمات الهواتف النقالة، واستخدام التواصل الاجتماعي بين السكان البالغين، ونسبة انتشار الدعاية عبر فيسبوك بين السكان البالغين، ومتوسط عدد حسابات التواصل الاجتماعي الشخصية التي يمتلكها كل شخص)، ووفقاً لهذا التقرير فقد بلغ عدد مستخدمي الشبكة العنكبوتية في الإمارات 9,732,158 مستخدماً في 2019. انظر: "الإمارات الأولى عالمياً في 6 قطاعات رقمية عام 2019"، https://www.albayan.ae/economy/local-market/2020-09-03-1.3765863 تاريخ التصفح: 9/3/2021م.

(2) في إمارة دبي فقط بلغ عدد البلاغات التي تلقتها إدارة المباحث الإلكترونية بشرطة دبي المتعلقة بالجرائم الإلكترونية خلال عام 2019 منذ إطلاق خدمة منصة ecrime والمعنية بتلقي بلاغات وشكاوى الجرائم المتعلقة بالإنترنت 9046 بلاغ، وتنوعت البلاغات بين جرائم التهديد والابتزاز الإلكتروني، واختراقات للمراسلات الإلكترونية، وبلاغات نصب واحتيال إلكتروني. وأسهمت إدارة المباحث الإلكترونية خلال عام 2020 في استرجاع 1277 حساب بريد إلكتروني لأشخاص تقدموا ببلاغات عبر منصة ecrime. انظر: https://www.albayan.ae/across-the-uae/news-and-reports/2020-05-16-1.3561505 تاريخ التصفح: 9/3/2021م.

مشكلة البحث:

تتمثل مشكلة البحث في أنه مع تطور الوسائل التكنولوجية والاتصالات وانتقالها إلى معلومات، ظهر ما يعرف بإتلاف المعطيات المعلوماتية، ومنها محتويات البريد الإلكتروني، وهو الأمر الذي يؤثر على الاستفادة من تلك المعطيات ويهدر قيمتها، حيث ينصب الإتلاف على إحداث الضرر بالبريد الإلكتروني وإعاقته عن أداء وظيفته، ويتم إتلاف محتويات البريد على نحو يجعلها غير صالحة للاستعمال، مما يخلق الاضطراب بين صفوف الأفراد والمؤسسات على حد سواء؛ لذلك جاءت مشكلة البحث للوقوف على مدى كفاية وكفاءة النصوص القانونية في التشريع الإماراتي في مواجهة جريمة الإتلاف لمحتويات البريد الإلكتروني؟ وكيف حاول المشرع توفير الحماية للبريد الإلكتروني وعدم الاعتداء عليه؟ وهل جاءت هذه النصوص مشتملة على كافة صور التجريم والعقاب الخاصة بإتلاف محتويات البريد الإلكتروني، أم أن الحاجة تقتضي إضافة نصوص قانونية جديدة تتماشى مع التطورات المستقبلية في وسائل تقنية المعلومات والبرمجيات المتنوعة؟ وإلى أي مدى نجح المشرع الإماراتي في وضع الجوانب الموضوعية لجريمة إتلاف محتويات البريد الإلكتروني؟

أهداف البحث:

يسعى هذا البحث الى:

1. تحديد مفهوم البريد الإلكتروني وطبيعته القانونية ومبررات حمايته من الإتلاف.
2. الوقوف على البنيان القانوني لجريمة إتلاف محتويات البريد الإلكتروني.
3. توضيح مدى معالجة المشرع الإماراتي للجوانب الموضوعية المتعلقة بحماية البريد الإلكتروني من إتلاف محتوياته عبر البرامج والتقنيات الحديثة.

منهجية البحث:

يعتمد الباحث في سبر أغوار هذا البحث على المنهج التحليلي، وذلك من خلال التعرض لنصوص التشريع الإماراتي التي عالجت الحماية الجنائية للبريد الإلكتروني من إتلاف محتوياته، ولا سيّما النصوص الواردة بقانون جرائم تقنية المعلومات الاتحادي؛ إذ إنّ دراسة النصوص القانونية وتحليلها تغدو ضرورة ملحة لتقييم موقف المشرع الإماراتي من هذا الموضوع.

خطة الدراسة:

سيتم تناول موضوعات هذا البحث من خلال المبحثين التاليين:

المبحث الأول: ماهية إتلاف البريد الإلكتروني ومبررات حمايته:

- المطلب الأول: مفهوم إتلاف البريد الإلكتروني.
- المطلب الثاني: مبررات حماية البريد الإلكتروني من الإتلاف.

المبحث الثاني: البنيان القانوني لجريمة إتلاف محتويات البريد الإلكتروني:

- المطلب الأول: أركان جريمة إتلاف محتويات البريد الإلكتروني.
- المطلب الثاني: العقوبات والتدابير المقررة لجريمة إتلاف محتويات البريد الإلكتروني.

الخاتمة

قائمة المراجع

المبحث الأول: ماهية إتلاف البريد الإلكتروني ومبررات حمايته

أصبح البريد الإلكتروني اليوم من الخدمات الأساسية التي تقدمها شبكة الإنترنت وتتعامل بها جميع المؤسسات والأفراد على حدٍ سواء للتواصل أو التعامل فيها بينهم دون الحاجة إلى قطع المسافات أو التواجد المادي، كونه وسيلة إلكترونية لتبادل المراسلات والبيانات والصور بين طرفين أو أكثر، فضلاً عن سهولة استعمال البريد الإلكتروني مقارنة بغيره من وسائل الاتصال.

ولقد أتاحت شبكة المعلومات الدولية "الإنترنت" العديد من الخدمات الإلكترونية التي يمكن استعمالها، ومنها خدمة البريد الإلكتروني، حيث أصبح بإمكان الأفراد والمؤسسات أن يتبادلوا الرسائل والمعلومات فيما بينهم وبتباعد المكان واختلاف الزمان من خلاله؛ إذ يتميز البريد الإلكتروني بالسرعة في نقل المعلومات؛ ولهذا أصبح من الوسائل الأساسية في الاتصال[1].

(1) حوراء موسى، الجرائم المرتكبة عبر وسائل التواصل الاجتماعي، دار النهضة العربية، القاهرة، 2018م، ص 33.

وللوقوف على ماهية إتلاف البريد الإلكتروني وبيان المبررات التقنية والقانونية لحمايته، سيتم تقسيم هذا المبحث كالتالي:

- **المطلب الأول: مفهوم إتلاف البريد الإلكتروني.**
- **المطلب الثاني: مبررات حماية البريد الإلكتروني من الإتلاف.**

المطلب الأول: مفهوم إتلاف البريد الإلكتروني

تتيح تقنية البريد الإلكتروني للأشخاص الذين لديهم حساباً استقبال وإرسال رسائل في وقت قصير من وإلى أي مكان في العالم، وقد تكون فورية، ويتيح للمستخدمين إرفاق ملفات وصور وفيديو أو وثائق إلكترونية أياً كان نوعها وطبيعتها ترسل مع الملف المرسل عبر البريد الإلكتروني[1]، ولذلك جرم المشرع الإماراتي فعل التعدي على البريد[2] والذي يحدث من خلال إغراقه بالرسائل، أو إيقافه عن العمل وتعطيله، أو إتلاف محتوياته، وهذا الاستحداث في التجريم من قبل المشرع الإماراتي يؤدي إلى حماية البريد الإلكترونيمن الاعتداء عليه أوالإضرار به.

وللوقوف على مفهوم إتلاف البريد الإلكتروني من كل جوانبه والتعرف على طبيعته القانونية، سيتم تناول هذا المطلب على النحو التالي:

(1) خالد ممدوح إبراهيم، حجية البريد الإلكتروني في الإثبات، دار الفكر الجامعي، الإسكندرية، 2010، ص 42.

(2) **والبريد الإلكتروني ليس نوعاً واحداً، ولكنه يتنوع إلى الآتي:**
النوع الأول: البريد الإلكتروني المباشر، وفيه يتصل الشخص المرسل مباشرة بمودم الشخص المستقبل، حيث يقوم مودم المرسل بتغيير الرسالة من الحالة الرقمية إلى نبضات تتجاوب مع خطوط الهاتف ومودم المستقبل الذي يقوم باستقبال هذه النبضات وإعطائها صيغة رقمية وتقوم برامج المعالجة الخاصة بالحاسب الآلي على استعادة الصيغة المقروءة للمراسلات، وتظل الرسالة في صيغة رقمية غير مقروءة عندما تكون الرسالة في حالة إرسال على خادم البريد الإلكتروني، وذلك إلى حين وصولها إلى مودم المستقبل واستلامها.
النوع الثاني: البريد الإلكتروني الخاص بالمؤسسات، وله حالتين: الأولى، نظام البريد الإلكتروني الداخلي للمؤسسة، وهذا النوع يتاح فقط التعامل به داخل مؤسسة واحدة، والثانية: البريد الإلكتروني غير الداخلي ويطلق عليها شبكة اكسترانت، وتتيح هذه الشبكة للمستخدمين من إمكانية وجود اتصال شبكي بين فروع المؤسسة الواحدة والإدارات والأقسام المختلفة داخل المؤسسة نفسها.
النوع الثالث: نظام مقدم خدمات الخط المفتوح، وهو نظام يقوم بموجبه مزود الخدمات بإعطاء كلمة مرور للمستخدم تمكنه من الدخول إلى النظام البريدي لدى مقدم الخدمات الذي يقدم هذه الخدمة بمقابل.
النوع الرابع: نظام مقدم خدمات الدخول إلى الإنترنت، ويقوم هذا النظام على اتصال بالإنترنت من خلال شبكة محلية تتصل بشبكات أكبر، ويكون لكل منها دور في إرسال البريد الإلكتروني، وتكون الرسالة بموجبة قابلة للتوصيل ما دام مزود دخول في مناطق الإرسال.
لمزيد من التوضيح انظر: خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الإسكندرية، 2010م، ص 117.

أولاً- تعريف البريد الإلكتروني:

إن مصطلح البريد الإلكتروني هو مصطلح مركب من مفردتين هما (البريد) و (الإلكتروني)، وفيما يلي نعرفهما وصولاً لوضع مفهوم شامل للبريد الإلكتروني.

(البريد) لغة يقصد به التواصل والتخاطب والتفاهم والتقارب بين المرسل والمرسل إليه، وقد قيل ما بين كل منزلين بريد والبريد المرسل على دواب البريد والجمع برد وبرد بريداً أرسله[1].

و(إلكتروني) اسم منسوب إلى إلكترون "Electron" وهي كلمة إنجليزية غير عربية، ويرتبط الإلكترون بالأجهزة والوسائل التي تؤدي وظائفها من خلال حركة الإلكترون وتحت تأثير المجالات الكهربائية والمغناطيسية[2]، وتتفق هذه التعريفات مع ما نصت عليه المادة (1) من المرسوم بقانون اتحادي رقم (5) لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات، حيث عرفت الإلكتروني بأنه: كل ما يتصل بالتكنولوجيا الكهرومغناطيسية أو الكهروضوئية أو الرقمية أو مؤتمتة أو ضوئية أو ما شابه ذلك، وتم تعريف الإلكتروني في المادة الأولى من قانون المعاملات والتجارة الإلكترونيةالاتحادي رقم (1) لسنة 2006 حيث نصت على أنه: "ما يتصل بالتكنولوجيا الحديثة ويكون ذا قدرات كهربائية أو رقمية أو مغناطيسية أو لاسلكية أو بصرية أو كهرومغناطيسية أو مؤتمتة أو ضوئية أو ما شابه ذلك".

وقد اختلف الفقه في إيراد تعريف موحد أو أسس معينة للبريد الإلكتروني؛ إذ جاءت أغلب التعاريف بمضمون الوظيفة التي يؤديها البريد الإلكتروني ومزاياه، حيث عرفه جانب من الفقه بأنه: "الطريقة التي من خلالها يسمح بتبادل الرسائل المطبوعة بين الأجهزة المتصلة بشبكة الإنترنت"[3]، **ويلاحظ على هذا التعريف** أنه لا يتضمن المزايا الأخرى التي يقوم بها البريد، ومنها إرسال واستقبال الوثائق والمستندات والحوالات التجارية والصور والفيديو وغيرها.

في حين عرفه جانب آخر من الفقه بأنه: "عبارة عن مستودع يحفظ الأوراق والمستندات شرط أن يتم تأمين هذا المستودع بعدم الدخول إليه من خلال نظام للتشفير أو كلمة مرور مؤمنة وغيرها من تقنيات الحماية التكنولوجية"[4]، وعرفه البعض بأنه:

(1) أبو الفضل جمال الدين بن محمد بن مكرم ابن منظور، لسان العرب، الجزء 3، دار صادر، بيروت، 2003، ص 56.

(2) سليمان محمد أحمد، طرق حماية التجارة الإلكترونية، دار الكتاب الجامعي، الإسكندرية، 2008، ص 16.

(3) عبد الفتاح حجازي، الحكومة الإلكترونية ونظامها القانوني، دار الفكر الجامعي، الإسكندرية، 2004، ص 172.

(4) محمد السيد عبد العاطي، الإنترنت وجوانبها القانونية، دار النهضة العربية، القاهرة، 2001، ص 118.

"الخدمة الأكثر استخداماً بين الخدمات كافة والتي تقدمها شبكة الإنترنت، حيث تتيح هذه الخدمة إمكانية الاتصال وتبادل الرسائل بين مستخدمي الشبكة على مدى 24 ساعة وبتكلفة الاتصال فقط"[1]، **ويلاحظ على هذا التعريف** أنه لا يواكب التطور في مجال التكنولوجيا، حيث إن البريد لم يعد الأكثر استخداماً بين الخدمات التي تقدمها الشبكة العالمية للمعلومات، لا سيما بعد ظهور وسائل التواصل الاجتماعي (واتساب، فيسبوك، تويتر، انستجرام، سناب شات) وغيرها من الوسائل الاخرى التي تتضمنها شبكة الإنترنت وأجهزة الهواتف الذكية.

وعرفه البعض بأنه: "وسيلة تبادل إلكترونية غير مباشرة للرسائل بين الأجهزة الإلكترونية"[2]، وعرفه البعض الآخر بأنه: وسيلة إنشاء الخطابات وإرسالها إلى شخص أو أكثر ويتم حفظ الرسالة على جهاز حاسوب بحيث يتم فتحها والتعامل معها"[3]، وعرفه جانب من الفقه بأنه: "وسيلة اتصال وتراسل إلكترونية سريعة يتم من خلالها إرسال واستلام كافة البيانات بين المرسل والمرسل إليه وتعتبر في الوقت ذاته صندوق لحفظ هذه البيانات والمستندات الخاصة بالمستخدم في ظل الحماية القانونية والتقنية اللازمة له لعدم تعرضه للاختراق أو التخريب"[4]، وعرفته الموسوعة الحرة العالمية للمعلومات "ويكيبيديا" بأنه: وسيلة لتبادل رسائل رقمية عبر شبكة الإنترنت أو شبكات حاسوبية متواصلة، ويتميز بالسرعة في إرسال الرسائل التي تتضمن نصاً مكتوباً أو صوتياً أو فيديو والصور والخرائط وإمكانية إرسال رسالة واحدة إلى العديد من المتلقين"[5].

وعرف المشرع الأمريكي في القانون الصادر عام 1986 بشأن خصوصية الاتصالات الإلكترونية، البريد الإلكتروني بأنه: "الوسيلة التي يتم بواسطتها نقل الرسائل الخاصة عبر الشبكة المعلوماتية عامة كانت أو خاصة وفي الغالب يتم كتابة المراسلات على أجهزةالحاسب الآلي ثم إرسالها إلكترونياً إلى جهاز مسؤول الخدمة، والذي يتولى بدوره تخزين الرسالة لديه حتى يتمكن المرسل إليه من استقبالها واستعادتها"، كما عرفه المشرع الفرنسي في القانون الخاص بالاقتصاد الرقمي لعام 2004 بأنه: "كل رسالة سواء كانت مكتوبة أو صوتية أو متعلق بها أصوات أو صور ويتم إرسالها عبر شبكة الاتصالات الإلكترونية العامة ويتم تخزينها في أحد خوادم شبكة الاتصالات أو في المعدات الخاصة

(1) عبد الهادي العوضي، الجوانب القانونية للبريد الإلكتروني، دار النهضة العربية، القاهرة، 2005، ص 13.

(2) خالد ممدوح إبراهيم، حجية البريد الإلكتروني في الإثبات، مرجع سابق، ص 42.

(3) جميل عبد الباقي الصغير، الإنترنت والقانون الجنائي، دار النهضة العربية، القاهرة، 2002، ص 115.

(4) عبدالله راشد اليماحي، إجراءات تفتيش نظم الحاسب الآلي، رسالة ماجستير، أكاديمية شرطة دبي، 2014م، ص 81.

(5) الموسوعة الحرة العالمية للمعلومات ويكيبيديا: ar.wikipedia.org/wiki – تاريخ الزيارة: 7/3/2021م.

بمزود الخدمة حتى يقوم هذا الأخير من استعادتها"[1].

ومن خلال الإطلاع على التشريعات العربية الخاصة بمواجهة جرائم تقنية المعلومات، يلاحظ أن أغلبها لم يتعرض لتعريف البريد الإلكتروني بشكل مباشر باستثناء قانون الإمارات العربي بشأن مكافحة الجرائم المعلوماتية وما في حكمها لعام 2004[2]، حيث نصت المادة الأولى منه على أن البريد الإلكتروني هو "نظام للتراسل باستخدام شبكات الحاسبات".

ويرى الباحث أن المشرع الإماراتي في المرسوم بقانون اتحادي رقم (5) لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات، قد توسع في شأن مكافحة تلك الجرائم بعدم ذكر مصطلح الحاسب الآلي أو البريد الإلكتروني على وجه الخصوص في المادة (1) من (التعريفات) وإنما جعلها عامة ومرتبطة بـ(الوسائل المعلوماتية) وأشار إلى أن تلك الوسائل بمثابة أدوات تستخدم لمعالجة البيانات الإلكترونية أوأداء العمليات المنطقية والحسابية، أو القيام بالوظائف التخزينية، وتشمل هذه الوسائل أي وسيلة موصلة أو مرتبطة بشكل مباشر بالحاسب الآلي وتتيح حفظ البيانات وسرعة إيصالها للآخرين، **ونستنتج من هذا التعريف** بأن كل وسائل الاتصال التقنية الحديثة وباختلاف تطبيقاتها الإلكترونية والذكية والمشابهة لها تدخل ضمن هذا التعريف، كما نتفق مع المشرع الإماراتي في التعريف الذي ذهب اليهلتضمين أي وسائل تقنية مشابه يمكن أن تستحدث في المستقبل.

ومن خلال التعريفات السابقة يتضح أنها لم تقدم تعريفاً جامعاً للبريد الإلكتروني، وقد جاءت أغلبها بصياغات مختلفة، وركزت على مضمون الوظيفة التي يؤديها البريد الإلكتروني ومزاياه، وعليه يمكن للباحث وضع تعريف للبريد الإلكتروني بأنه: عبارة عن مستودع للبريد ومربوط بشبكة الإنترنت مؤمن من خلال نظام التشفير أو رمز سري يمكن من خلاله نقل واستلام المعلومات والبيانات بين طرفين أو أكثر في وقت قياسي دون أهمية للموقع الجغرافي.

ثانياً- تعريف إتلاف البريد الإلكتروني

يقصد بإتلاف محتويات البريد الإلكتروني إتلاف المكونات المنطقية أو"التخريب

(1) Emmanuel Zidafamor, (2018), A -Term Paper- On Computer Crime and Cyber attacks, American University of Nigeria, Department of Computer Science and Software Engineering, P82.

(2) اعتمده مجلس وزراء العدل العرب التابع لجامعة الدول العربية في دورته التاسعة عشر بموجب القرار رقم 495/ د 19 في تاريخ 8/10/2003، ومجلس وزراء الداخلية العرب في دورته الحادية والعشرين بموجب القرار رقم 417/ د 21 في تاريخ 4/6/2004م.

المنطقي أو تدمير نظم المعلومات البريد الإلكتروني، ويقصد به في المفهوم التقليدي جعل الشيء غير صالح للاستعمال كلياً أو جزئياً بإعدام صلاحيته أو تعطيله ووقفه عن العمل بصورة كلية أو جزئية، أما في مجال البريد الإلكتروني فيمكن تعريفه بمحو وتشويه محتويات البريد الإلكتروني بواسطة البرامج والوسائل الفنية المخصصة لذلك، على نحو يجعل من البريد غير صالح للاستخدام[1].

ومن الواضح أن إتلاف نظم المعلومات يمكن أن يقع في صورتين، أولهما الصورة التقليدية، وثانيهما الصورة المعلوماتية، مع ما يحصل بينهما من تداخل[2]:

1. **الإتلاف التقليدي:** ويقصد به وقوع أفعال الإتلاف على المكونات المادية للحاسب من أجهزة ووحدات إدخال وإخراج وشاشات وكابلات وأقراص ممغنطة وأدوات الربط والتوصيل وما شابه ذلك، ولا شك في أن أفعال الإتلاف هذه تكيف على أنها جريمة عادية تخضع للنصوص التقليدية في قانون العقوبات، إذ لا شك أن هذه المكونات المادية لها صفة الأموال المادية والعائدة للغير، مما يسمح بإخضاعها للنصوص التقليدية في قانون العقوبات.

2. **الإتلاف المعلوماتي:** ويقصد به وقوع الإتلاف على المعلومات والبيانات المخزنة داخل الحاسب الآلي أو شبكة الإنترنت بما يحقق جريمة الإتلاف المعلوماتي، وهي الصورة المقصودة في هذا البحث، إتلاف محتويات البريد الإلكتروني، ويلاحظ أنه لا يمكن حصر وسائل إتلاف المعلومات، ولا يمكن التنبؤ بها مستقبلاً، لما تشهده من تطور متسارع وتنوع واضح، لا سيما وأن الاكتشافات في هذا المجال باتت مما لا يمكن إيقافه أو السيطرة عليه، وعلى العموم، فإن أبرز هذه الوسائل الفنية والتقنية هي: الفيروسات الضارة والبرامج التخريبية والخبيثة وغيرها، والفيروس برنامج كأي برنامج تطبيقي آخر، ولكنه يصمم بواسطة أحد المخربين بهدف إحداث أكبر ضرر ممكن في النظام بعد ربطه بالبرامج الأخرى، وله القدرة على التكاثر حتى يبدو وكأنه يتوالد ذاتياً مما يتيح له القدرة على استهداف البرامج الأخرى في الحاسب ومواقع أخرى في الذاكرة بهدف تدميرها، والفيروس في المجال المعلوماتي هو برنامج تتم كتابته ليقوم بنسخ ونشر نفسه ذاتياً دون تعاون المالك أو المستخدم للجهاز، كما يعرف بأنه برنامج يصيب البرامج الأخرى، حيث يعدل فيها عن طريق إدخال نسخة منه فيها يقوم بإنتاجها ولديه القدرة على تطوير نفسه خلال عملية إعادة إنتاج نفسه، ويمكن الانتشار في النظام المعلوماتي أو

(1) عبد الهادي العوضي، الجوانب القانونية للبريد الإلكتروني، مرجع سابق، ص 76.

(2) عمار عباس الحسيني، جرائم الحاسوب والإنترنت، مرجع سابق، ص 183.

الشبكة أو البريد الإلكتروني ليسبب في البريد ومحتوياته تغييرات تحكمية تدميرية، مما يؤدي إلى إتلاف محتوياته[1].

ثالثاً- الطبيعة القانونية للبريد الإلكتروني:

إن وظيفة البريد الإلكتروني لا تقتصر فقط على العمليات التقنية والفنية، بل يرافقها أيضاً العديد من الجوانب، ولذلك يقتضي البحث في الطبيعة القانونية للبريد الإلكتروني، حيث اختلف الفقه في مسألة التكييف القانوني للبريد الإلكتروني، وبذل الفقه مساعيه للوصول إلى إيراد تكييف قانوني صحيح له، ومن ثم يكون خاضعاً إلى تنظيم قانوني محدد، فالبريد الإلكتروني وإن كان عبارة عن تكوين فني يمكن من خلاله التواصل مع الآخرين، فإنه لا يخلو من بعض الدلالات القانونية التي يجب تحليلها لمحاولة الوصول إلى تكييفه القانوني، وسنوضح ذلك كالتالي:

1. التكييف القانوني للبريد الإلكتروني وفق الأفكار القانونية:

اتجه جانب من الفقه[2] إلى تكييف البريد الإلكتروني وفق الأفكار القانونية، حيث يذهب اتجاه من الفقه إلى اعتباره عنصراً من عناصر الشخصية القانونية، واعتبره رأي آخر بأنه عبارة عن فكرة قانونية مستقلة، ويشير الرأي الأول إلى أن عناصر الشخصية القانونية تتمثل في: الاسم والموطن، وعليه فإن هذا الاتجاه يجعل عنوان البريد صورة جديدة لاسم الشخص أو موطنه، ويدلل بذلك أن اسم البريد الإلكتروني الشخصي يتميز به صاحبه عن غيره، وبذلك يمكن تمييز المستخدم عن غيره.

وثمة تساؤل يتم طرحه في هذا الشأن: مع أي صورة من صور الاسم يتشابه عنوان البريد الإلكتروني، هل يتشابه مع الاسم العائلي أم يتشابه مع الاسم المستعار؟

يرى البعض[3] أن الاسم المدني يميز الاسم العائلي في العالم الحقيقي، إلا أنه في العالم الافتراضي، وإن كانت تسمية البريد الإلكتروني قد تكون لمستخدمه، فهو يحدده فقط داخل هذا العالم الافتراضي، فاسم البريد الإلكتروني يكون على وفق إرادته واختياره ولا يشترط أنه يكون مفروضاً على الشخص أو المستخدم تطبيقاً لقواعد النسب، أما بالنسبة للاسم المستعار فهو كل اسم يطلقه الشخص على نفسه بإرادته واختياره ليستر شخصيته الحقيقية فيما يتعلق بممارسته بعض الأنشطة أو لتحقيق بعض الأمور التي يبتغيها، وقد

(1) حسين علي محمد حطاب، الحماية الجزائية للبريد الإلكتروني، مرجع سابق، ص 119.

(2) جلال الزعبي، أسامة المناعسة: جرائم تقنية نظم المعلومات الإلكترونية، دار الثقافة للنشر، عمان، 2010م، ص 81.

(3) خالد ممدوح إبراهيم، حجية البريد الإلكتروني في الإثبات، مرجع سابق، ص 68.

يكون لمستخدم البريد الإلكتروني أكثر من اسم مستعار سواء بتغيير هذا الاسم أو باستخدام اسم مستعار في كل نشاط يريد فيه أن يستر شخصيته الحقيقية.

ويظهر الاختلاف بين عنوان البريد الإلكتروني والاسم المستعار في أن القانون قد يمنع بعض الفئات أن تتخذ اسماً مستعاراً لها كالقضاة والمحامين والأطباء والمسؤولين وغيرهم من الأفراد، ومع ذلك فإن استخدام الاسم المستعار لغير هؤلاء على شبكة الإنترنت هو أمر غير محظور ومن ثمة يمكنهم الدخول إلى مواقع شبكة الإنترنت المختلفة، وإذا ما كان عنوان البريد الإلكتروني يتخذ اسم مستعار فإنه لا بدّ وأن يكون اسم مشروع وغير منتحل[1].

يتضح مما تقدم أن العنوان الذي يدل على البريد الإلكتروني قد يأخذ اسم المستخدم نفسه في بعض الأحيان ووظيفته في أحيان أخرى، وعندئذ لا يمكن اعتباره نوعاً جديداً للاسم، ومن ثم لا يمكن أن يكون خاضعاً لأحكامه القانونية، وعليه فإنه وفق هذا الاتجاه فإن البريد الإلكتروني يعد بمثابة فكرة قانونية مستقلة بذاتها، وبالإمكان أن يستند في تطبيق أحكامه إلى مجموعة من المصادر مثل وثائق الجهات المختصة بالتسجيل والأحكام القضائية، وحكم الواقع.

2. التكييف القانوني للبريد الإلكتروني وفق المفاهيم التقنية:

اتجه رأي آخر في الفقه[2] إلى محاولة إعطاء تكييف قانوني للبريد الإلكتروني وفق مفاهيم تقنية وفنية، حيث اتجه إلى محاولة تشبيه البريد الإلكتروني برقم الهاتف أو رقم الهوية، ويستند هذا الرأي إلى أنه إذا رجعنا لعنوان البريد الإلكتروني لوجدناه عبارة عن مجموعة من الحروف والأرقام التي تكتب من قبل المستخدم والتي لا بدّ منها حتى يمكنه الدخول إلى بروتوكول الاتصال.

كما ذهب رأي آخر من الفقه[3] إلى وصف عنوان البريد الإلكتروني بأنه عنصرٌ من عناصر الملكية الصناعية، إذ ذهب هذا الاتجاه إلى تشبيه البريد الإلكتروني بالعلامة التجارية والاسم والعنوان التجاري للمؤسسات والشركات، ومن ثم يكون البريد الإلكتروني خاضعاً للتنظيم والأحكام القانونية لهذه العناصر القائمة، وبالتالي يكون عنوان البريد

(1) هلالي عبد اللاه أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية، دار النهضة العربية، القاهرة، 2007م، ص237.

(2) منى كامل تركي، الحماية الجنائية لحق الخصوصية في جرائم التصوير والتسجيل بدون إذن، دراسة مقارنة، دار النهضة العربية، القاهرة، 2019م، ص 187.

(3) محمد علي العريان، الجرائم المعلوماتية، دار الجامعة للنشر، الإسكندرية، 2013م، ص 117.

الإلكتروني من العناصر المعنوية، باعتباره هو الجانب الرئيس الذي تقوم عليه المعاملات التجارية، ومن ثم يكون لهذا العنوان وزن تجاري خاص به، لا سيما في الوقت الحاضر في ظل تزايد الاعتماد على شبكة الإنترنت في المعاملات التجارية.

ومن خلال ما سبق، يخلص الباحث إلى أن البريد الإلكتروني ذو طبيعة قانونية خاصة، كونه وسيلة للمراسلات الخاصة، ولا أهمية للوسائل التي يتم من خلالها نقل تلك المراسلات، كما أن الرسالة الإلكترونية كما عرفتها المادة (1) من قانون المعاملات والتجارة الإلكترونية الاتحادي رقم (1) لسنة 2006 من أنها تعد من قبيل الرسائل الخاصة وفق القانون، وعليه فإن المشرع يوفر لها الحماية ضمن نطاق حماية الحق في الخصوصية المعلوماتية، وبالتالي عدم الجواز لغير صاحب البريد الإلكتروني أن يطلع على محتواه لكون ذلك يعد انتهاكًا لسريته، وكذلك التعدي على حرمة المراسلات الخاصة، وقد وفر المشرع الإماراتي الحماية للبريد الإلكتروني من خلال نصوص جزائية خاصة للجرائم التي ترتكب ضد البريد الإلكتروني في المرسوم بقانون اتحادي رقم (5) لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات، سواء من خلال إتلاف محتوياته أو إغراقه بالرسائل أو توقيفه وتعطيله عن العمل.

المطلب الثاني: مبررات حماية البريد الإلكتروني من الإتلاف

حرص المشرع الإماراتي على تجريم كل فعل من شأنه أن يمثل تعدياً على حق الإنسان في حرمة محادثاته ومراسلاته، وعلة تجريم هذا التعدي تتمثل في حماية كل شخص في أن تكفل لحياته حرمتها وأن تحاط بسياج من السرية، فلا ينفذ منه شخص إلا برضاء من صاحب هذا الحق، وأهم مظهرين لهذا الحق أراد المشرع الإماراتي حمايتهما أولا حماية المحادثات الخاصة وثانيا حماية المراسلات بما فيها المستندات والوثائق المرسلة عبر البريد الإلكتروني، وجدير بالذكر أن التعدي على البريد الإلكتروني سواء بالاختراق أو التعطيل والايقاف عن العمل أو سرقة محتوياته، يعتبر عدواناً خطيراً على حقوق الإنسان لا سيما الحق في الحياة الخاصة، ويعتبر البريد الإلكتروني من عناصر الحق في الحياة الخاصة، فالرسالة الإلكترونية المرسلة عبر البريد الإلكتروني تعد من الأمور المتعلقة بالحياة الخاصة للأفراد لما تتضمنه هذه المراسلات من أسرار[1].

ومن المستقر عليه فقهاً أن لكل إنسان الحق في تمتعه بخصوصية مراسلاته، وعليه تعد المراسلات الإلكترونية الشخصية عبر البريد الإلكتروني من عناصر الحق في الخصوصية أو الحياة الخاصة، حيث يتم من خلالها تبادل بعض المعلومات والأسرار والأفكار المتعلقة بأشخاص طرفي البريد الإلكتروني دون حيطة أو حذر، بعيداً عن شبهة التلصص عليها، ومن هنا أضفى المشرع الجنائي الحماية على هذه المحادثات الإلكترونية حفاظاً على

حقوق وحريات الأشخاص[1].

ولقد أورد المشرع الإماراتي تطبيقات للحق في الخصوصية في الدستور وقانون العقوبات الاتحادي أو أي قانون من القوانين الجزائية الأخرى، لا سيما الخصوصية المتعلقة بسرية المحادثات والمراسلات البريدية أو المحادثات الهاتفية أو غيرها من وسائل الاتصال، وهكذا يبدو أن حماية الحق في الخصوصية للأفراد لا يمكن أن يتحقق إلا بسن التشريعات التي تحمي سرية المراسلات والمحادثات الخاصة للأفراد[2]، الأمر الذي يلزم الغير باحترام السرية سواء كانت سرية المراسلات أو المحادثات الخاصة، كما حرصت معظم دساتير العالم على كفالة حماية قانونية لحق الإنسان في سرية مراسلاته واتصالاته الشخصية، وليس معنى عدم النص عليها من قبل بعض الدساتير عدم إقرارها، وإنما كل ما هنالك هو أن هذه الدساتير لا تجد نفسها في حاجة إلى النص عليها؛ نظراً لأن هذه الحقوق تستمد أصلها من القانون الطبيعي نفسه وما نص غالبية الدساتير عليها، إلا تأكيداً لهذه الحقوق وليس إقرارها لها، ومما لا شك فيه أن هذه الحماية الدستورية تعد من أقوى الضمانات لحماية هذا الحق، إذ أنها ترفع هذا الحق من الحقوق العادية إلى الحريات العامة التي يكفلها الدستور[3].

ومن المؤكد أن السياسة التشريعية تساهم في صياغة القوانين إلى حد كبير عن طريق تحديد المصالح الواجب حمايتها، كما أنها تحدد أهداف التشريع والخطوط العريضة التي يجب إتباعها، فمن خلال النصوص التجريمية في المرسوم بقانون اتحادي بشأن مكافحة جرائم تقنية المعلومات، ومنها جريمة الاعتداء على الحق في خصوصية المراسلات المعلوماتية، تتحدد المصلحة الواجب حمايتها، وتعد المصلحة هي حكمة التجريم، وهي المعيار الذي يستعين به الشارع في مرحلتي التقنين والتطبيق، وكل تجريم يتضمن في ثناياه عدواناً على مركز قانوني تحميه قاعدة التجريم، فالمصلحة دائماً هي مناط التجريم والعقاب أو كما يقال علة التجريم، ويعد التجريم بمثابة أعلى مراتب الحماية التي يضيفها المشرع على أي من المصالح التي تهم المجتمع[4].

(1) محمود عبد الرحمن محمد، نطاق الحق في الحياة الخاصة – دراسة في القانون الوضعي والشريعة الإسلامية، دار النهضة العربية، القاهرة، 2006، ص 11.

(2) عبد الرازق الموافي، شرح قانون مكافحة جرائم تقنية المعلومات الإماراتي، الكتاب الأول، معهد دبي القضائي، 2016م، ص 118.

(3) محمود أحمد طه، التنصت والتلصص على سرية الاتصالات الشخصية بين التجريم والمشروعية، مرجع سابق، ص 76.

(4) هلالي عبد اللاه أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية، مرجع سابق، ص 136.

ولا ريب أن كل شكل من أشكال الاعتداء على المراسلات التي يحتويها البريد الإلكتروني، لا سيما في إتلاف محتوياته يقابله انتهاك حق من حقوق الإنسان، فالاعتداء على خصوصية مراسلات البريد الإلكتروني يتعارض مع الحق في الخصوصية، والحق في الحرية الشخصية[1].

وتتنوع مبررات حماية البريد الإلكتروني من الإتلاف، إلا أنه سيتم التركيز على المبررات التقنية والقانونية، وذلك على النحو التالي:

1. المبررات التقنية لحماية البريد الإلكتروني من الإتلاف:

يلاحظ أن الحماية التقنية في أغلب الأحيان ليست كافية لحماية وتأمين البريد الإلكتروني، وعليه يتم الاعتداء عليه بمختلف البرامج والتقنيات التي تخترقه أو تتلف محتوياته أو غيرها من أساليب الاعتداء، ويمكن إجمال أهم المبررات التقنية في تحول الحكومات من تقليدية إلى حكومات إلكترونية وذكية، حيث تعتبر دولة الإمارات واحدة من الدول الأكثر استخداماً لتكنولوجيا المعلومات في تطوير أداء العمل للجهات الحكومية، والنهوض بكفاءة وجودة الخدمات وتسهيل طرق الحصول عليها بالنسبة للمواطنين، الذين هم الهدف والغاية النهائية لأي عمل حكومي أو تنموي، وبعد أن كانت دولة الإمارات العربية المتحدة من الدول السباقة في اعتماد نموذج الحكومة الإلكترونية وحققت تقدماً كبيراً في ذلك[2]، ففي 22/5/2013 تم الإعلان عن مبادرة "الحكومة الذكية" من أجل توفير الخدمات للجمهور حيثما كانوا وعلى مدار الساعة، وتسريع وتيرة التحول الذكي في القطاع الحكومي على المستويين المحلي والاتحادي، وتشجيع الجمهور على تبني واستخدام الخدمات الذكية، ويركز التحول إلى الحكومة الذكية في دولة الإمارات العربية المتحدة على الاستخدام الاستراتيجي لأحدث إصدارات تكنولوجيا المعلومات وفي مقدمتها التطبيقات الذكية، بهدف تطوير طرق العمل في المؤسسات الحكومية، وذلك للوصول لأقصى درجات رضا المتعاملين، وبالتعاون الفعال مع جميع الجهات ذات الصلة، ويتم ذلك عبر توفير وسائل تواصل سلسة وتفاعلية وذكية تعمل في أي وقت وأي مكان، عبر العديد من الأجهزة، حيث تتضمن الحكومة الذكية إجراء تحسينات مميزة على إجراءات العمل وطريقة عمل الموظفين، وتوفير الخدمات الأكثر ملاءمة للجمهور وفقاً لاحتياجاتهم[3]، وتتركز الأهداف الإستراتيجية لحكومة الإمارات الذكية في الآتي[4]:

---

(1) حوراء موسى، الجرائم المرتكبة عبر وسائل التواصل الاجتماعي، مرجع سابق، ص 251.

(2) دليل الحكومة الذكية، هيئة تنظيم الاتصالات، الإصدار الثاني، أغسطس 2018، ص 21.

(3) آفاق الخدمات الحكومية الذكية في العالم العربي، سلسلة بحوث القمة الحكومية، فبراير 2018، ص 36.

(4) مبادرة حكومة الإمارات الذكية، https://u.ae/ar-ae/about-the-uae/digital-uae/uae-mgovern-

1. المساهمة الفعالة في تحقيق رؤية دولة الإمارات وصولا إلى العالمية.
2. تعزيز القدرة التنافسية لدولة الإمارات.
3. تعزيز الدور الحكومي والابتكارات المجتمعية في مجال التقنيات الذكية بتسهيل وسائل الوصول للخدمات الحكومية بجودة عالية ومن أي موقع وعلى مدار الساعة.
4. تخفيض تكاليف عمليات المؤسسات الحكومية من خلال تطوير وسائل وأدوات تقديم المعلومات والمنتجات والخدمات.
5. تعزيز التعاون بين المؤسسات المختلفة.
6. تسهيل أعمال الأفراد والمؤسسات بما يساهم في دعم الاقتصاد والمجتمع المعرفي.
7. الانتقال من رضا الأفراد والمؤسسات إلى إسعادهم.
8. المساهمة في رفع القدرة الإنتاجية للقوى العاملة والمؤسسات الحكومية.

ووفقاً لنتائج التحول الذكي في دولة الإمارات للحكومة الإلكترونية، فقد وصلت نسبة الإنجاز للخدمات الإلكترونية اليومية للمتعاملين الى 96,6 % في عام 2020م[1].

وحرصاً من حكومة دولة الإمارات العربية المتحدة على إيجاد بيئة تشريعية تنظم تعاملاتها والتجارة الإلكترونية والذكية، فقد بذلت الجهود اللازمة لتحديث الأطر والقوانين التشريعية في هذا المجال، وذلك من خلال إصدار المرسوم بقانون اتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات، ولمواكبة التطورات التقنية فقد أصدر المشرع عدة تشريعات أخرى، ومنها قانون تنظيم قطاع الاتصالات رقم (3) لسنة 2003، وقانون المعاملات والتجارة الإلكترونية رقم (1) لسنة 2006، كما تحرص الحكومة على ضمان استمرارية تأمين البيانات والمعلومات بصورة متكاملة ضد المخاطر، وتتطلع رؤية الإمارات 2021 إلى أن تصبح الدولة الأولى عالمياً في عدة مؤشرات معلوماتية[2] منها: (مؤشر البنية التحتية للاتصالات) و(مؤشر الخدمات الإلكترونية والذكية)، كما وضعت الدولة عدة أدلة إرشادية لحماية البيانات وتأمينها.

---

ment-initiative تاريخ التصفح: 10/3/2021م.

(1) الموقع الإلكتروني لهيئة تنظيم الاتصالات في دولة الإمارات، https://www.tra.gov.ae/ar/about-tra/information-and-egovernment-sector.aspx تاريخ التصفح: 10/3/2021م.

(2) وفقاً لتقارير التنافسية العالمية حققت دولة الإمارات المركز (7) في المؤشر العالمي للبنية التحتية للاتصالات لعام 2020، والمركز (8) في مؤشر الخدمات الإلكترونية والذكية. انظر: الموقع الإلكتروني للأجندة الوطنية لرؤية الإمارات: www.vision2021.ae تاريخ الزيارة: 11/3/2021م.

ومن خلال ما تقدم، فإذا أردنا تطبيق مفهوم الحكومة الإلكترونية الذكية وتوفير كافة متطلباتها التكنولوجية والإدارية والقانونية، وفي ظل تشريعات جزائية من شأنها ضمان الحماية القانونية لكل ما يتعلق بإجراءات ومعاملات الحكومة الإلكترونية الذكية، فإن البريد الإلكتروني يعد من أهم الوسائل في الحكومة الإلكترونية، وهو عامل أساسي لنجاح تلك التجربة.

2. المبررات القانونية لحماية البريد الإلكتروني من الإتلاف:

إن من أهم وأبرز صور حماية البيانات الواردة في البريد الإلكتروني هو تشفيرها، وغالباً ما يتم ذلك قبل إرسالها عبر الشبكة لضمان سلامة وصولها دون التعرض لأي عملية تجسس أو قرصنة أو تحريف للمضمون، وبالتالي تستمد المعلومة سريتها من طبيعة مضمونها؛ إذ لا تكون معروفة أو متداولة، لأنها لن تكون سرية، وستكون صالحة للتداول العام من دون أن يستأثر بها شخص أو مجموعة أشخاص متخصصين في اختراق البريد الإلكتروني[1].

ولقد أظهرت الدراسات أن مجرمي تقنية المعلومات غالباً ما يعملون في دول تفتقر لنظم تشريعية صارمة أو وعي كاف حول هذا الموضوع؛ ولذلك أصدرت دولة الإمارات عدة قوانين لمواجهة الجرائم الإلكترونية، ومنها القانون الاتحادي رقم (5) لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات، وذلك لمواجهة الجرائم المرتكبة عبر شبكات ووسائل تقنية المعلومات[2].

واتخذت دولة الإمارات العربية المتحدة العديد من الإجراءات والتدابير لتعزيز أمنها الإلكتروني، ومنها تنفيذ شبكة إلكترونية اتحادية FEDNET تسمح بالتوصيل البيني، وتبادل البيانات بين جميع الجهات المحلية والاتحادية في الدولة، وتعزز قنوات التواصل فيما بينها باستخدام قواعد بيانات آمنة، حيث توفر الشبكة بيئة أمن متعددة الطبقات تضمن أعلى مستويات الأمان في البنية التحتية اعتماداً على الترميز متعدد البروتوكولات (MPLS) وتتيح ربطاً آمناً بالإنترنت لكافة الجهات الحكومية الاتحادية عبر مزود مزدوج لخدمة الإنترنت[3].

---

(1) حسين علي محمد حطاب، الحماية الجزائية للبريد الإلكتروني – دراسة مقارنة، رسالة ماجستير، كلية القانون، جامعة القادسية، العراق، 2017م، ص 82.

(2) إمام حسنين خليل عطا الله، الحماية الجنائية لوسائل تقنية المعلومات في التشريعات العربية (الإمارات نموذجاً)، مركز الدراسات والاستطلاعات، وزارة الداخلية، أبوظبي، 2016م، ص 121.

(3) الموقع الإلكتروني لبوابة حكومة الإمارات: https://u.ae/ar-ae/about-the-uae/science-and-technology/key-sectors-in-science-and-technology/information-and-communication-

كما أصدرت هيئة تنظيم الاتصالات بدولة الإمارات الدليل الإرشادي لنظام ضمان أمن المعلومات في الدولة لتعزيز بيئة رقمية آمنة وموثوقة في ظل التطور التكنولوجي وتزايد التهديدات السيبرانية المواكبة له، بما في ذلك تهديدات نشطاء القرصنة الإلكترونية[1].

ويلاحظ أن الدول دائماً ما تشرع القوانين الجزائية لسن الجرائم والعقوبات لحماية حقوق وحريات الافراد وتسعى لتحقيق أهدافها في الردع العام والخاص، ومع ذلك فهي بحاجة دائمة إلى تحديث تشريعاتها لمواجهة المستحدث من الجرائم، لا سيما جرائم الاعتداء على البريد الإلكتروني.

المبحث الثاني: البنيان القانوني لجريمة إتلاف محتويات البريد الإلكتروني

من الجرائم التي تقع على أنظمة المعلومات، ومنها البريد الإلكتروني، جريمة الإتلاف المعلوماتي، ولا شك أن لإتلاف محتويات البريد الإلكتروني خطورة واضحة، كونه يؤدي إلى العديد من الخسائر المادية، فضلاً عما يعكسه من خطورة إجرامية تقنية احترافية، وصعوبات فنية وقانونية تتعلق بالإثبات، كما تعكس في أحيان كثيرة دوافع خبيثة، والتي تعمل على تدمير وإتلاف وتعطيل نظم المعلومات بأكملها[2]، ولا يمكن حصر وسائل إتلاف محتويات البريد، ولا يمكن التنبؤ بها مستقبلا، نظراً لما تشهده وسائل وتقنيات المعلومات والبرمجيات ووسائل الاتصالات من تطورات واضحة[3].

وللوقوف على البنيان القانوني لجريمة إتلاف محتويات البريد الإلكتروني، سيتم تقسيم هذا المبحث على النحو الآتي:

- **المطلب الأول: أركان جريمة إتلاف محتويات البريد الإلكتروني.**
- **المطلب الثاني: العقوبات والتدابير المقررة لجريمة إتلاف محتويات البريد الإلكتروني.**

---

technology تاريخ الزيارة: 12/3/2021م.

(1) الإستراتيجية الوطنية للأمن السيبراني في دولة الإمارات: https://www.tra.gov.ae/ar/national-cybersecurity-strategy.aspx تاريخ الزيارة: 12/3/2021م.

(2) عبد الرازق الموافي، شرح قانون مكافحة جرائم تقنية المعلومات الإماراتي، مرجع سابق، ص 89.

(3) عمار عباس الحسيني، جرائم الحاسوب والإنترنت، مرجع سابق، ص 178.

المطلب الأول: أركان جريمة إتلاف محتويات البريد الإلكتروني

ينصب الإتلاف على إحداث الضرر بالبريد الإلكتروني وإعاقته عن أداء وظيفته، حيث يتم إتلاف محتوياته على نحو يجعلها غير صالحة للاستعمال، مما يخلق الاضطراب بين صفوف الأفراد والمؤسسات على حد سواء[1]، وبالاطلاع على المادة (10) من قانون مكافحة جرائم مكافحة تقنية المعلومات والتي نصت على أنه: (.... وتكون العقوبة الحبس والغرامة أو إحدى هاتين العقوبتين عن أي فعل عمدي يقصد به إغراق البريد الإلكتروني بالرسائل.... أو إتلاف محتوياته).

يتضح من نص المادة السابقة أن محل الجريمة الجنائية هنا هو البريد الإلكتروني، ويقصد به المراسلات والوثائق المكتوبة أو المصورة وغير ذلك، التي يتم إرسالها واستقبالها من خلال نظام اتصالات بريدي إلكتروني ينطوي على جمل مختصرة، ويمكن إضافة مرفقات عبارة عن كلمات أو مواد فيلمية أو أية وثائق ومستندات إلكترونية أخرى ترسل مع الملف المرسل عبر البريد الإلكتروني، حيث تتيح تقنية البريد الإلكتروني للأشخاص الذين لديهم بريداً إلكترونياً استقبال وإرسال رسائل في وقت قصير من وإلى أي مكان في العالم، وقد تكون بصورة فورية، ويتيح البريد الإلكتروني لمستخدميه إرفاق ملفات ووثائق أياً كان نوعها وطبيعتها[2].

ويتضح للباحث من خلال نص المادة السابقة أن المشرع الإماراتي أكد على تجريم الاعتداء على البريد الإلكتروني الذي يحدث من خلال إتلاف محتوياته من بيانات ومعلومات ووثائق، وهذا التجريم يؤكد على حرص المشرع على حماية البريد الإلكتروني من الاعتداء عليه.

ومن الواضح أن هذه الجريمة وكأي جريمة أخرى تتطلب لقيامها تحقق الركنين المادي والمعنوي، وهو ما سنوضحه كالتالي:

الفرع الأول: الركن المادي لجريمة إتلاف محتويات البريد الإلكتروني

لم يحدد المشرع الإماراتي وسيلة معينة يتحقق بها إتلاف محتويات البريد الإلكتروني، وبالتالي تتنوع الوسائل التي تشكل اعتداءً على البريد الإلكتروني، ويقصد بالركن المادي لجريمة إتلاف محتويات البريد الإلكتروني كل فعل أو امتناع عن فعل يؤدي إلى الإضرار بالمعلومات المخزنة في البريد الإلكتروني والتي تؤدي إلى هدر أو إنقاص قيمتها وتسبب

(1) حسين علي محمد حطاب، الحماية الجزائية للبريد الإلكتروني، مرجع سابق، ص 115.

(2) عبد الهادي العوضي، الجوانب القانونية للبريد الإلكتروني، مرجع سابق، ص 81.

ضرر بالآخرين، فالسلوك الإجرامي في هذه الجرائم لا بدّ أن يتم من خلال أجهزة الحاسب الآلي أو شبكة الإنترنت وما في حكمها[1].

ويكون إتلاف محتويات البريد الإلكتروني من خلال ممارسة أي سلوك يترتب عليه هذا الإتلاف، وذلك من خلال استخدام شفرات ضارة ومدمرة وفيروسات تخريبية تنتقل من حاسب آلي إلى آخر، ومن بريد إلكتروني إلى آخر، أو أي وسيلة إلكترونية أخرى تحقق النتيجة ذاتها الممثلة في إتلاف محتويات البريد الإلكتروني، ويكون ذلك عن طريق التعديل غير المشروع للبيانات والمعلومات التي يحتوي عليها البريد الإلكتروني أو تدميرها ومحوها أو الإدخال غير المشروع عليها[2].

وجدير بالذكر أن المسلك الذي ذهب إليه أغلب التشريعات – ومنها التشريع الإماراتي – التي تناولت هذه الجريمة لم يتطلب لقيامها أن تكون البيانات محل الإتلاف مختصة بنوع معين أو قطاع معين، بخلاف بعض التشريعات التي تطلبت مثل هذا التخصيص، ومنها مثلاً القانون الفيدرالي في الولايات المتحدة لعام 1996 الذي قصرها على الحاسبات الآلية التابعة للحكومة، والأمر ذات في قانون العقوبات الاسترالي لعام 1989 الذي قصر الحماية الجنائية في جريمة الإتلاف المعلوماتي على المعلومات التي تخص حاسبات الكومنولث، ويستوي في الدخول إلى النظام المعلوماتي والمؤدي إلى الإتلاف، أن يكون هذا الدخول قد حصل بشكل مباشر أو غير مباشر[3].

يتضح مما تقدم أن المشرع الإماراتي لم يحدد وسيلة معينة لارتكاب جريمة إتلاف البريد الإلكتروني، أي أن الجريمة من الممكن أن تقع بأي وسيلة من الوسائل المساعدة على إحداث الضرر للبيانات والمعلومات التي يحتوي عليها البريد الإلكتروني وإتلافها عن طريق استخدام شفرات ضارة بالمعلومات أو فيروسات تخريبية تنتقل من حاسب آلي آخر ومن بريد إلكتروني إلى آخر أو ملفات ارتباطية مدمرة تؤدي إلى محو محتويات البريد الإلكتروني، ويشير البعض[4] إلى الركن المادي في جريمة إتلاف محتويات البريد الإلكتروني يأتي في ثلاث صور هي:

1. **التعديل غير المشروع للبيانات والمعلومات التي يحتوي عليه البريد الإلكتروني:** وهي أكثر صور الإتلاف شيوعاً، ويقصد به استخدام إحدى وظائف الحاسب

(1) خالد ممدوح إبراهيم، حجية البريد الإلكتروني في الإثبات، مرجع سابق، ص 156.

(2) عمار عباس الحسيني، جرائم الحاسوب والإنترنت، مرجع سابق، ص 191.

(3) جميل عبد الباقي الصغير، الإنترنت والقانون الجنائي، مرجع سابق، ص 224.

(4) عبد الهادي العوضي، الجوانب القانونية للبريد الإلكتروني، مرجع سابق، ص 83.

الآلي لإجراء تغيير غير مشروع للبيانات والمعلومات التي يحتوي عليها البريد الإلكتروني، أو هي الأفعال التي تؤدي إلى عدم قابلية البيانات والمعلومات التي يحتوي عليها البريد للاستعمال على النحو المعد له.

2. **تدمير البيانات والمعلومات التي يحتوي عليها البريد الإلكتروني:** وتتمثل هذه الصورة في محو البيانات والمعلومات تماماً أو إخفائها بحيث لا يمكن الوصول إليها دون محوها.

3. **الإدخال غير المشروع على البيانات والمعلومات التي يحتوي عليها البريد الإلكتروني:** حيث قد يتم ذلك في شكل إدخال برنامج خبيث للبريد الإلكتروني أو تدوين بيانات غير صحيحة بغرض إعاقته على أداء وظيفته.

ويلاحظ أن هذه الجريمة تعد من جرائم الخطر وليست من جرائم الضرر، حيث لم يتطلب لقيامها تتحقق نتيجة إجرامية ضارة تلحق بالمصلحة العامة أو المصلحة الخاصة أو بكليهما، وقد أظهر المشرع ذلك في المادة (10) من المرسوم بقانون اتحادي رقم (5) لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات وتعديلاته، وذلك في قوله: "وتكون العقوبة الحبس والغرامة أو إحدى هاتين العقوبتين عن أي فعل عمدي يقصد به إغراق البريد الإلكتروني..... أو إتلاف محتوياته"، أي أن جريمة إتلاف محتويات البريد الإلكتروني تتم بمجرد ارتكاب سلوك معين بقصد اتلاف البريد الإلكتروني حتى ولو لم تتحقق نتيجة مادية كعنصر من ركنها المادي، وبالتالي تعتبر هذه الجريمة من جرائم الخطر، ويتضح ذلك من خلال نص المادة سالفة الذكر، حيث تقوم الجريمة ويعاقب عليها بمجرد تعمد الجاني بأي فعل قاصداً إتلاف محتويات البريد الإلكتروني سواءٌ تحققت النتيجة وهي الإتلاف أو لم تتحقق، كأن يقوم الجاني بإرسال رسالة إلى البريد الإلكتروني الخاص بالمجني عليه تحتوي على ملف فايروسات مدمرة بقصد إتلافه إلا أن النتيجة لم تحقق وهي الإتلاف ففي مثل هذه الحالة تقوم الجريمة ويعاقب الجاني وفقاً لنص المادة 10 سالفة الذكر.

ولكي يتحقق الركن المادي لجريمة إتلاف محتويات البريد الإلكتروني لا بدّ من وجود علاقة سببية بين السلوك الإجرامي والنتيجة الإجرامية وهي الإتلاف إذا تحققت بناءً على السلوك الإجرامي للجاني؛ إذ يجب أن تثبت العلاقة ما بين السلوك الإجرامي والنتيجة الإجرامية وهي إتلاف محتويات البريد الإلكتروني، بحيث يحرم مستخدم البريد الإلكتروني من الاستفادة بما يحتويه البريد الإلكتروني الخاص به، ويكون ذلك عن طريق التعديل غير المشروع للبيانات والمعلومات التي يحتوي عليها البريد الإلكتروني أو تدميرها أو الإدخال غير المشروع عليها[1].

(1) عبد الرازق الموافي، شرح قانون مكافحة جرائم تقنية المعلومات الإماراتي، مرجع سابق، ص 92.

وباعتبار جريمة إتلاف البريد الإلكتروني من جرائم الخطر بانه ليس من المتصور الشروع فيها، حيث أنه بمجرد قيام الجاني بالسلوك الاجرامي قاصداً الإتلاف تتحقق الجريمة تامة ويعاقب عليها بالعقوبة المقررة لجريمة الاتلاف، وبالتالي اذا قام الجاني بإرسال رسائل عبر البريد الإلكتروني تحتوي فايروسات بقصد إتلاف البريد الإلكتروني للجاني إلا أن النتيجة لم تتحقق وهي الإتلاف، في مثل هذه الحالة نكون أمام جريمة تامة وليس شروع في الجريمة مما يستوجب العقاب على الجريمة التامة.

الفرع الثاني: الركن المعنوي لجريمة إتلاف محتويات البريد الإلكتروني

تعد جريمة إتلاف محتويات البريد الإلكتروني من الجرائم العمدية، حيث يتطلب لقيام الركن المعنوي فيها، تحقق القصد الجنائي بعنصريه العلم والإرادة؛ إذ يجب أن يعلم الجاني بأن سلوكه يؤدي إلى إتلاف محتويات البريد الإلكتروني، وأن تتجه إرادته إلى ارتكاب السلوك المذكور مريداً تحقيق آثاره الجنائية[1]، وبخلاف ذلك، فإن اعتقد الفاعل بناءً على أسباب معقولة أنه يعتدي على معلومات تعود له، فإن عنصر العلم ينتفي لديه، كمن يعتقد أنه يقوم بإتلاف بيانات من البريد الإلكتروني ويعتقد أنه يعود له مع ندرة هذا الفرض، وأيضاً ينتفي العلم عندما يرسل الجاني رابطاً إلكترونيًّا من بريد إلكتروني إلى بريد إلكتروني لشخص آخر، ويحتوى هذا البريد الإلكتروني على ملفات بها فيروسات ضارة تسبب تلفاً لمحتويات البريد الإلكتروني للشخص الآخر في حالة تم فتحها، وذلك دون أن يعلم الجاني بإصابة هذه الملفات بالفيروسات الضارة لديه.

ويلزم لقيام القصد الجنائي أن تتجه إرادة الجاني إلى ارتكاب السلوك الإجرامي المتمثل في فعل إتلاف البريد الإلكتروني بما يحتويه من بيانات ومعلومات ووثائق إلكترونية وغيرها، سواء تم ذلك الإتلاف بشكل كلي أو جزئي، بمعنى أن تتجه إرادة الجاني إلى تحقيق النتيجة الإجرامية التي تتمثل في الإتلاف[2]، وفي حالة انتفاء الإرادة ينتفي القصد الجنائي.

ويثار لدينا تساؤل حول طبيعة القصد الجنائي: هل تقوم الجريمة بتوفر القصد الجنائي العام أم يشترط لقيامها توافر قصد جنائي خاص؟ باستقراء نص المادة (10) من قانون مكافحة جرائم تقنية المعلومات يتضح أنه يشترط القصد الجنائي الخاص بالإضافة الى القصد العام، حيث اشترط لقيام الجريمة تعمد الجاني القيام بأي فعل بقصد إتلاف محتويات البريد الإلكتروني، وبالتالي يتضح لنا أن المشرع قد اشترط نية خاصة، وهي نية إتلاف محتويات البريد الإلكتروني.

(1) عبد الهادي العوضي، الجوانب القانونية للبريد الإلكتروني، مرجع سابق، ص 89.

(2) هلالي عبد اللاه أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية، مرجع سابق، ص 181.

المطلب الثاني: العقوبات والتدابير المقررة لجريمة إتلاف محتويات البريد الإلكتروني

سوف نتناول في هذا المطلب الجزاءات التي قررها المشرع الاتحادي لجريمة إتلاف محتويات البريد الإلكتروني وذلك على النحو التالي:

الفرع الأول: عقوبات جرائم إتلاف محتويات البريد الإلكتروني:

أولاً- العقوبات الأصلية

العقوبات الأصلية هي الجزاء الأساسي للجريمة، ولا توقع العقوبة الأصلية إلا إذا نطق بها قاضي الموضوع وحدد نوعها ومقدارها، وتستمد وصفها من أنها تكون العقاب الأصلي أو الأساسي المباشر للجريمة والتي توقع منفردة بغير أن يكون القضاء بها معلقاً على الحكم بعقوبة أخرى[1].

وفي شأن جريمة إتلاف محتويات البريد الإلكتروني لقد نص المادة (10) من المرسوم بقانون اتحادي رقم (5) لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات وتعديلاته، على عقوبة الحبس والغرامة أو إحدى هاتين العقوبتين، وبتطبيق القواعد العامة يتضح لنا أن المشرع الإماراتي قد جرم إتلاف البريد الإلكتروني بوصف الجنحة، وبالتالي سوف تكون عقوبة الحبس مدة لا تقل عن شهر ولا تزيد عن ثلاث سنوات، والغرامة التي لا تقل عن ألف درهم ولا تجاوز ثلاثمائة ألف درهم، كما أن المشرع أعطى للقاضي سلطة تقديرية في اختيار إحدى هاتين العقوبتين.

وباستقراء النص السابق يلاحظ أن المشرع لم يفرق في التجريم أو العقاب بينما إذا كان البريد الإلكتروني شخصي أو كان البريد الإلكتروني تابع لجهة حكومية عامة، أو ما إذا كان مالك البريد الإلكتروني شخصاً عادياً أو موظفاً عاماً، حيث جعل المشرع العقوبة واحدة وهي الحبس والغرامة أو إحداهما، وعلى الرغم من أن المشرع أعطى للقاضي سلطة واسعة في هذا الأمر في أنه يطبق الحد الأدنى للعقوبة سواء كانت الحبس أو الغرامة أو يطبق الحد الأقصى.

ويرى الباحث أنه كان من الأجدر أن يميز المشرع في العقوبة على حسب مضمون محتويات البريد الإلكتروني محل الجريمة، بمعنى إذا كان البريد الإلكتروني ينطوي على معلومات سرية وهامة تخص المجني عليه، لا سيما إذا كان المجني عليه شخصية عامة في

(1) علي محمود حمودة، الوجيز في الأحكام العامة لقانون العقوبات الاتحادي، النظرية العامة للجزاء الجنائي، أكاديمية شرطة دبي، 2019م، ص 172.

الدولة أو جهة حكومية، ويحتوي البريد الإلكتروني على بيانات ومعلومات هامة قد تضر بمكانة واعتبار هذه الشخصية الهامة، أو بيانات ومعلومات هامة قد تمس الجهة الحكومية أو أمن الدولة الداخلي أو الخارجي، بحيث تشدد العقوبة، بعكس ما إذا كان محتوى البريد الإلكتروني لشخص عادي أو أي جهة أخرى غير عامة بحيث تطبق العقوبة المنصوص عليها دون تشديد.

وإن كان المشرع قد اعتبر جريمة إتلاف البريد الإلكتروني من جرائم الخطر وعاقب عليها بمجرد ارتكاب الجاني للسلوك بقصد الإتلاف وإن لم تتحقق النتيجة، إلا أنه لم يفرق في العقوبة بين تحقق النتيجة وهي الإتلاف لمحتوى البريد الإلكتروني وعدم تحققها، حيث يرى الباحث أن يشدد المشرع في العقوبة في حال تحققت النتيجة وهي الإتلاف.

ثانياً- العقوبات التكميلية

يقصد بالعقوبة التكميلية تلك العقوبة التي تكمل العقوبة الأصلية، ولا يتصور توقيعها بمفردها، وإنما يتوقف تطبيقها على نطق القاضي بها، أي لا يجوز تنفيذها على المحكوم عليه إذا لم ينص عليها في الحكم، ولذلك لم يجعل المشرع أمر هذه العقوبات متحققاً بقوة القانون، وإنما اشترط للحكم بها أن ينطق بها القاضي صراحة في الحكم الذي يصدره[1].

كما تعرف العقوبات التكميلية بأنها تلك العقوبات التي تنطق بها المحكمة بالإضافة إلى العقوبة الأصلية[2]، وتتضمن الحرمان من بعض الحقوق والمزايا بصفة تكميلية[3]، وكذلك المصادرة[4].

ووفقاً لنص المادة (41) من المرسوم بقانون اتحادي رقم (5) لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات، يلاحظ أن المشرع أضاف بعض العقوبات التكميلية لجريمة إتلاف محتويات البريد الإلكتروني، إذ نصت المادة (41) من المرسوم بقانون على وجوب الحكم

(1) جميل عبد الباقي الصغير، الإنترنت والقانون الجنائي، مرجع سابق، ص 115.

(2) علي محمود حمودة، الوجيز في الأحكام العامة لقانون العقوبات الاتحادي، النظرية العامة للجزاء الجنائي، مرجع سابق، ص 176.

(3) تنص المادة (80) من قانون العقوبات على أنه: (للمحكمة عند الحكم في جناية بالحبس أن تأمر بحرمان المحكوم عليه من حق أو مزية أو أكثر مما نص عليه في المادة 75 وذلك لمدة لا تقل عن سنة ولا تزيد على ثلاث سنوات تبدأ من نهاية تنفيذ العقوبة أو انقضائها لأي سبب آخر).

(4) تنص المادة (82) من قانون على أنه: (تحكم المحكمة عند الحكم بالإدانة بمصادرة الأشياء والأموال المضبوطة التي استعملت فيها أو كان من شأنها أن تستعمل فيها أو كانت محلا لها أو التي تحصلت من الجريمة، فإذا تعذر ضبط أيا من تلك الأشياء أو الأموال حكمت المحكمة بغرامة تعادل قيمتها، وذلك كله دون الإخلال بحقوق الغير حسن النية).

في جميع الأحوال بمصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في هذه الجريمة.

والأصل أن المصادرة عقوبة فرعية تكميلية جوازيه، للمحكمة سلطة تقديرية في الحكم بها أو غير ذلك، وفي بعض الحالات تكون وجوبية ويلزم أن ينطق بها القاضي في حكمه، وقد نص قانون العقوبات الاتحادي على المصادرة في المادة (82) منه، وهي عقوبة تكميلية لا توقع إلا بحكم من القاضي، كما أنها عقوبة مشتركة بين جميع الجرائم وفقاً لهذا النص، وكذلك نصت المادة (41) من المرسوم بقانون اتحادي بشأن مكافحة جرائم تقنية المعلومات على هذه العقوبة واعتبرتها وجوبية بنصها على (مع عدم الإخلال بحقوق الغير حسني النية يحكم في جميع الأحوال بمصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا المرسوم بقانون أو الأموال المتحصلة منها...)، ويتضح من نص المادة (82) من قانون العقوبات الاتحادي أن المصادرة الجوازية عقوبة تكميلية بالمعنى الدقيق، وفي الحالة الوجوبية تكون تدبيراً وقائياً[1].

ولا يقضي بالمصادرة إلا في حالة وقوع جريمة، وبناءً على ذلك لا مصادرة إذا كان السلوك لا يخضع لنص تجريم أو يلحق به سبب إباحة، فالقاعدة أنه لا عقوبة ولا تدبير إلا من أجل فعل يعد جريمة[2]، **وإن كان البعض قد يرى أنه كان** يمكن الاكتفاء بالنص العام في المادة (82) من قانون العقوبات الاتحادي دون الحاجة إلى نص خاص في قانون مكافحة جرائم تقنية المعلومات، **إلا أن الباحث يرى** أن المشرع قد أحسن صنعاً في وضع هذا النص الخاص في قانون مكافحة جرائم تقنية المعلومات سواء جعلها وجوبية أو جوازية أو قام باستبعادها، حيث يتبين من نص المادة (41) من قانون مكافحة جرائم تقنية المعلومات أن المصادرة وجوبية على جميع الجرائم المنصوص عليها فيه، ومن هنا كانت الحاجة إلى النص الخاص وعدم الاكتفاء بالنص العام.

الفرع الثاني: التدابير الاحترازية المقررة لجريمة إتلاف محتويات البريد الإلكتروني

توجد مجموعة من التدابير الاحترازية التي يجوز للمحكمة الحكم بها على مرتكبي جريمة إتلاف محتويات البريد الإلكتروني، نتناول منها ما يلي:

أولاً- إغلاق المحل أو الموقع:

نصت المادة (41) من قانون مكافحة جرائم تقنية المعلومات على تدبير من التدابير السالبة للحقوق والتدابير المادية، وهو إغلاق المحل التي يجوز للمحكمة الحكم بها لارتكاب

(1) عبيد صالح، سياسة المشرع الإماراتي لمواجهة الجرائم الإلكترونية، مجلة الفكر الشرطي، مركز بحوث الشرطة، الشارقة، العدد 95، 2015م، ص 133.

(2) جميل عبد الباقي الصغير، الإنترنت والقانون الجنائي، مرجع سابق، ص 237.

جريمة إتلاف محتويات البريد الإلكتروني، حيث نصت على أنه: "... كما يحكم بإغلاق المحل أو الموقع الذي يرتكب فيه أي من هذه الجرائم، وذلك إما إغلاقاً كلياً أو للمدة التي تقدرها المحكمة".

ويقصد بإغلاق المحل منع ممارسة النشاط الذي كان يمارس فيه قبل صدور الحكم، وفي حالة الجريمة محل الدراسة، إذا كان مرتكب الجريمة يمارس نشاط له علاقة بتقنية المعلومات، كأن يكون لديه مؤسسة للحاسب الآلي والبرمجيات أو يمتلك موقعاً إلكترونياً أو بريداً إلكترونياً، وبسبب هذا النشاط قام بارتكاب جريمته، فإن المحكمة تقضي بإغلاق هذا المحل أو الموقع الذي يرتكب فيه أي من هذه الجرائم، وذلك إما إغلاقاً كلياً أو للمدة التي تقدرها المحكمة[1]، ومن خلال صياغة المادة (41) يتضح لنا بأن الإغلاق لم يرد على سبيل الجواز وإنما جاء على سبيل الوجوب، ومن ثم يترتب على ذلك بطلان الحكم إذا لم يحكم القاضي بالإغلاق كعقوبة تكميلية للعقوبة الأصلية.

ولقد نظم المشرع الاتحادي أحكام إغلاق المحل في المادة (128) من قانون العقوبات الاتحادي، والتي تنص على أنه فيما عدا الحالات الخاصة التي ينص فيها القانون على الإغلاق يجوز للمحكمة عند الحكم بمنع شخص من ممارسة عمله وفقاً للمادة (126) أن تأمر بإغلاق المحل الذي يمارس فيه هذا العمل وذلك لمدة لا تقل عن شهر ولا تزيد على سنة[2].

ثانياً- الوضع تحت الإشراف أو المراقبة أو الحرمان من استخدام تقنية المعلومات:

نصت المادة (43) من المرسوم بقانون اتحادي رقم (5) لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات على أن: (مع عدم الإخلال بالعقوبات المنصوص عليها في هذا المرسوم بقانون يجوز للمحكمة أن تأمر بوضع المحكوم عليه تحت الإشراف أو المراقبة أو حرمانه من استخدام أي شبكة معلوماتية أو نظام المعلومات الإلكتروني، أو أي وسيلة تقنية معلومات أخرى...).

ويستفاد من نص هذه المادة أن القاضي يتمتع بسلطة تقديرية بالنسبة للتدابير المذكورة – الوضع تحت الإشراف أو المراقبة أو الحرمان من استخدام تقنية المعلومات – يقضي بها أو لا يقضي، فإن حكمه يكون صحيحاً، لأنها جوازيه، والسلطة التقديرية للقاضي تكون من حيث الحكم بالتدبير ومن حيث مدته، وتوقع هذه التدابير بالإضافة للعقوبات المنصوص عليها في هذا المرسوم بقانون، فتوقيع التدابير لا يمنع من تطبيق العقوبة الأصلية[3].

(1) عبد الرازق الموافي، شرح قانون مكافحة جرائم تقنية المعلومات الإماراتي، مرجع سابق، ص 91.

(2) محمد السعيد عبد الفتاح، الوجيز في شرح قانون العقوبات الاتحادي لدولة الإمارات، الآفاق المشرقة، الشارقة، ط3، 2020، ص 336.

(3) عبدالله راشد اليماحي، إجراءات تفتيش نظم الحاسب الآلي، مرجع سابق، ص 94.

الخاتمة

مع تطور وسائل تكنولوجيا الاتصالات، ظهر ما يعرف بإتلاف المعطيات المعلوماتية، ومنها محتويات البريد الإلكتروني، وهو الأمر الذي يؤثر على الاستفادة من تلك المعطيات ويهدر قيمتها؛ إذ يَنصَبّ الإتلاف على إحداث الضرر بالبريد الإلكتروني وإعاقته عن أداء وظيفته وعلى نحو يجعله غير صالح للاستخدام، مما يخلق الاضطراب بين صفوف الأفراد والمؤسسات على حد سواء، **ومن خلال ما جاء في البحث تم التوصل إلى النتائج والتوصيات الآتية:**

أولاً- النتائج:

1. تعد جريمة إتلاف محتويات البريد الإلكتروني إحدى أبرز جرائم الاعتداء على الكيان المعنوي للحاسب الآلي، ناهيك على أنها لا تختلف عن الجرائم المعلوماتية الأخرى الواقعة على الأموال من حيث انطوائها على اعتداء غير مشروع على حق الملكية، ومهما تنوعت أساليب الاعتداء، إلا أنها تنصب في وعاء واحد، وهي إتلاف البيانات المخزنة في البيئة الافتراضية.

2. تبين أن البريد الإلكتروني ذو طبيعة قانونية خاصة، كونه وسيلة للمراسلات الخاصة، وقد وفر لها القانون الحماية ضمن نطاق حماية الحق في الخصوصية؛ ومن ثم عدم الجواز لغير صاحب البريد أن يطلع على محتواه لكون ذلك يعد انتهاك سرية وحرمة المراسلات الخاصة، وقد وفر المشرع الإماراتي الحماية للبريد الإلكتروني من خلال نصوص جزائية خاصة للجرائم التي ترتكب ضد البريد الإلكتروني في المرسوم بقانون اتحادي رقم (5) لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات وتعديلاته، سواء من خلال إتلاف محتوياته أو إغراقه بالرسائل أو توقيفه وتعطيله عن العمل.

3. أكد المشرع الإماراتي على تجريم الاعتداء على البريد الإلكتروني الذي يحدث من خلال إغراقه بالرسائل أو إيقافه وتعطيله أو إتلاف محتوياته من بيانات ومعلومات ووثائق، وهذا التجريم يؤكد على حرص المشرع الإماراتي على حماية البريد الإلكتروني من الاعتداء عليه، ولعل علة التجريم هذه تكمن في كون ما للبريد الإلكتروني من العديد من الفوائد للأفراد والمؤسسات على حدٍ سواء، لذا يجب الحرص عليه وعلى أداء وظائفه نحو الأفضل وحمايته مما بشأنه الإضرار به.

4. لم يحدد المشرع الإماراتي وسيلة معينة لارتكاب جريمة إتلاف البريد الإلكتروني، أي أن الجريمة من الممكن أن تقع بأي وسيلة من الوسائل المساعدة على إحداث

الضرر للبيانات والمعلومات التي يحتوي عليها البريد الإلكتروني وإتلافها عن طريق استخدام شفرات ضارة بالمعلومات أو فيروسات تخريبية تنتقل من حاسب آلي آخر ومن بريد إلكتروني إلى آخر أو ملفات ارتباطية مدمرة تؤدي إلى محو محتويات البريد الإلكتروني.

5. تعد جريمة إتلاف محتويات البريد الإلكتروني من الجرائم العمدية، ومن ثم يتطلب لقيام الركن المعنوي فيها تحقق القصد الجنائي الخاص بالإضافة الى القصد الجنائي العام بعنصريه العلم والإرادة، إذ يشترط علم الجاني المعلوماتي بأن سلوكه يؤدي إلى تحقق النتيجة المتمثلة في إتلاف محتويات البريد الإلكتروني، وأن تتجه إرادته إلى ارتكاب السلوك المذكور مريداً تحقيق آثاره الجنائية، بالإضافة إلى القصد الجنائي الخاص والمتمثل بقيام الجاني بفعل الاعتداء بقصد إتلاف محتويات البريد الإلكتروني.

6. لم يفرق المشرع في العقوبة فيما إذا كان البريد الإلكتروني عاماً أو خاصاً.

7. لم يفرق المشرع الإماراتي في العقوبة المقررة لجريمة اتلاف محتويات البريد الإلكتروني بين ارتكاب الجريمة وتحقق النتيجة وبين ارتكابها وعدم تحقق النتيجة.

8. أضاف المشرع الإماراتي بعض العقوبات التكميلية لجريمة إتلاف محتويات البريد الإلكتروني، إذ نصت المادة (41) من المرسوم بقانون اتحادي بشأن مكافحة جرائم تقنية المعلومات على وجوب الحكم في جميع الأحوال بمصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في هذه الجريمة، كما نص المشرع على عدة تدابير احترازية يجوز للمحكمة الحكم بها على مرتكبي الجريمة، ومنها: (إغلاق المحل أو الموقع الذي ارتكبت فيه جريمة الإتلاف، وضع الجاني تحت الإشراف أو المراقبة أو الحرمان من استخدام تقنية المعلومات).

ثانياً- التوصيات:

1. كان من الأجدر أن يميز المشرع في العقوبة المنصوص عليها في المادة (10) من قانون مكافحة جرائم تقنية المعلومات[1]، وذلك على حسب مضمون محتويات البريد الإلكتروني محل الجريمة، بمعنى إذا كان ينطوي على معلومات سرية ومهمة تخص المجني عليه سواء أكانت شخصية أو تخص مؤسسة حكومية،

(1) نص المشرع الإماراتي في المادة (10) من قانون مكافحة جرائم تقنية المعلومات وتعديلاته، على عقوبة الحبس أو الغرامة أو إحدى هاتين العقوبتين لجريمة إتلاف محتويات البريد الإلكتروني.

وجب تشديد العقوبة، بعكس ما إذا كانت تنطوي على مثل ذلك، كما لو كان البريد الإلكتروني يستخدم في المراسلات العادية ويخلو من أي أسرار أو معلومات مهمة، وفي هذه الحالة توقع العقوبة المناسبة لجسامة الفعل.

2. نناشد المشرع الإماراتي بضرورة وضع آلية قانونية تعاقدية بين مستخدمي الهاتف المتحرك ومزودي الخدمة في الدولة التي توفر تلك الخدمة، تكون هدفها حماية سرية البريد الإلكتروني، وخاصة وأن تطور تقنيات الهاتف المتحرك وانتشاره أصبح أكثر انتهاكاً لسرية الأفراد، كالهواتف المتحركة الذكية التي تتميز بخصائص تقنية متعددة، وأن تشمل هذه الآلية جميع العاملين في مؤسسات الاتصالات في حال انتهاكهم للبريد الإلكتروني الشخصي.

3. نوصي المشرع الإماراتي بان يفرق في العقوبة بتعديل الفقرة الأخيرة من المادة (10) من قانون مكافحة جرائم تقنية المعلومات في حال ارتكاب الجريمة وتحقق النتيجة وهي الإتلاف لمحتوى البريد الإلكتروني، وبين ارتكاب الجريمة وعدم تحقق النتيجة، بحيث يكون النص على النحو التالي ((وتكون العقوبة الحبس الذي لا تقل مدته عن سنة والغرامة التي لا تقل عن 50 ألف درهم إذا تحققت النتيجة في الجرائم السابقة)).

4. نوصي بتحديد مدة التدابير الاحترازية الجوازية في المرسوم بقانون اتحادي رقم (5) لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات وتعديلاته، بأن يكون لها حد أدنى وحد أقصى، ويقترح الباحث أنه يجب النص على أن لا يقل الحرمان عن شهر ولا أن يزيد على سنة في الجنح، إذ إن تنفيذ تدبير الحرمان من استخدام وسائل تقنية المعلومات على أرض الواقع وفقاً لما هو منصوص عليه في المادة (126) من قانون العقوبات الاتحادي ستتبعه الكثير من الإجراءات التعقيدية، لا سيما وأنه في ظل حياتنا المعاصرة لا يتخيل أن تقوم الحياة اليومية دون استخدام لوسائل تقنية المعلومات المختلفة، كما أن تطبيق مثل هذا التدبير يعد أمراً يصعب تطبيقه لإمكانية التحايل باستخدام شبكات ووسائل تقنية معلومات تعود لأشخاص آخرين.

قائمة المصادر والمراجع:

أولاً: المراجع العربية:

إبراهيم، خالد ممدوح (2010). حجية البريد الإلكتروني في الإثبات. دار الفكر.

إبراهيم، خالد ممدوح (2010). فن التحقيق الجنائي في الجرائم الإلكترونية. دار الفكر العربي.

أحمد، سليمان محمد (2008). طرق حماية التجارة الإلكترونية. دار الكتاب الجامعي.

أحمد، هلالي عبد اللاه (2007). الجوانب الموضوعية والإجرائية لجرائم المعلوماتية. دار النهضة العربية.

الإستراتيجية الوطنية للأمن السيبراني في دولة الإمارات: https://www.tra.gov.ae/ar/national-cybersecurity-strategy.aspx تاريخ الزيارة: 12/3/2021م.

استرجاع 1277 حساب بريد إلكتروني لأشخاص تقدموا ببلاغات عبر منصة ecrime لشرطة دبي: انظر: https://www.albayan.ae/across-the-uae/news-and-reports/2020-05-16-1.3561505 تاريخ التصفح: 9/3/2021م.

آفاق الخدمات الحكومية الذكية في العالم العربي (2018). سلسلة بحوث القمة الحكومية.

تركي، منى كامل (2019). الحماية الجنائية لحق الخصوصية في جرائم التصوير والتسجيل بدون إذن، دراسة مقارنة. دار النهضة العربية.

تقرير الحالة الرقمية لعام 2020 «الإمارات الأولى عالمياً في 6 قطاعات رقمية عام 2019»، https://www.albayan.ae/economy/local-market/2020-09-03-1.3765863 تاريخ التصفح: 9/3/2021م.

حجازي، عبد الفتاح (2004). الحكومة الإلكترونية ونظامها القانوني. دار الفكر الجامعي.

الحسيني، عمار عباس (2017). جرائم الحاسوب والإنترنت. منشورات زين الحقوقية.

حطاب، حسين علي محمد (2017). الحماية الجزائية للبريد الإلكتروني – دراسة مقارنة [رسالة ماجستير، جامعة القادسية]. https://doi.org/10.37138/1425-032-001-016

حمودة، علي محمود (2019). الوجيز في الأحكام العامة لقانون العقوبات الاتحادي، النظرية العامة للجزاء الجنائي. أكاديمية شرطة دبي.

الزعبي، جلال والمناعسة، أسامة (2010). جرائم تقنية نظم المعلومات الإلكترونية. دار الثقافة للنشر.

صالح، عبيد (2015). سياسة المشرع الإماراتي لمواجهة الجرائم الإلكترونية. مجلة الفكر الشرطي، مركز بحوث الشرطة، (95).

الصغير، جميل عبد الباقي (2002). الإنترنت والقانون الجنائي. دار النهضة العربية.

طه، محمود أحمد (2018). التنصت والتلصص على سرية الاتصالات الشخصية بين التجريم والمشروعية. دار الفكر والقانون.

عبد العاطي، محمد السيد (2001). الإنترنت وجوانبها القانونية. دار النهضة العربية.

عبد الفتاح، محمد السعيد (2020). الوجيز في شرح قانون العقوبات الاتحادي لدولة الإمارات (ط3). الآفاق المشرقة.

العريان، محمد علي (2013). الجرائم المعلوماتية. دار الجامعة للنشر. https://doi.org/10.21608/mbse.2013.144722

عطا الله، إمام حسنين خليل (2016). الحماية الجنائية لوسائل تقنية المعلومات في التشريعات العربية (الإمارات نموذجاً). مركز الدراسات والاستطلاعات، وزارة الداخلية.

العوضي، عبد الهادي (2005). الجوانب القانونية للبريد الإلكتروني. دار النهضة العربية.

القاسمي، إبراهيم محمد (2018). جرائم الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات الإلكترونية في التشريع الإماراتي [رسالة ماجستير، جامعة الإمارات].

مبادرة حكومة الإمارات الذكية، https://u.ae/ar-ae/about-the-uae/digital-uae/uae-mgovernment-initiative تاريخ التصفح: 10/3/2021م.

محمد، محمود عبد الرحمن (2006). نطاق الحق في الحياة الخاصة – دراسة في القانون الوضعي والشريعة الإسلامية. دار النهضة العربية.

الموافي، عبد الرازق (2016). شرح قانون مكافحة جرائم تقنية المعلومات الإماراتي، الكتاب الأول. معهد دبي القضائي.

موسى، حوراء (2018). الجرائم المرتكبة عبر وسائل التواصل الاجتماعي، دراسة مقارنة. دار النهضة العربية.

الموقع الإلكتروني لبوابة حكومة الإمارات: https://u.ae/ar-ae/about-the-uae/science-and-technology/key-sectors-in-science-and-technology/information-and-communication-technology تاريخ الزيارة: 12/3/2021م.

الموقع الإلكتروني للأجندة الوطنية لرؤية الإمارات: www.vision2021.ae تاريخ الزيارة: 11/3/2021م.

الموقع الإلكتروني لهيئة تنظيم الاتصالات في دولة الإمارات، https://www.tra.gov.ae/ar/about-tra/information-and-egovernment-sector.aspx تاريخ التصفح: 10/3/2021م.

الموسوعة الحرة العالمية للمعلومات ويكيبيديا: ar.wikipedia.org/wiki – تاريخ الزيارة: 7/3/2021م.

اليماحي، عبدالله (2014). إجراءات تفتيش نظم الحاسب الآلي [رسالة ماجستير، أكاديمية شرطة دبي].

ثانياً: المراجع الأجنبية:

Zidafamor, E. (2018). *A -Term Paper- On Computer Crime and Cyber attacks*. American University of Nigeria, Department of Computer Science and Software Engineering.

الترجمة الصوتية لمصادر ومراجع اللغة العربية: Romanized Arabic References:

'ibrāhym khālida mamdūḥa 2010). ḥujjiyyata albarydi al'ilikturwniyyi fī al'ithbāti dāru alfikri

'ibrāhym khālida mamdūḥa 2010). fanna al-taḥqīqi aljinā'iyyi fī aljarā'imi al'ilikturwniyyati dāru alfikri al'arabiyyi

a'aḥamdun salīmāni muḥammada 2008). ṭaraqa ḥimāyatu al-tijārati al'ilikturwniyyati dāru alkitābi aljāmi'iyyi

a'aḥamdun halāaliyya 'abdi alilāha 2007). aljawāniba almawḍū'iyyata wa-l-'ijrā'iyyata lijarā'ima alma'lūmātiyyati dāru al-nahḍati al'arabiyyati

al'istrātījiyyatu alwaṭaniyyatu lil-'ā'amna al-sybrāny fī dawlati al'imārāti https:// www. tra. gov. ae / ar / national- cybersecurity- strategy. aspx tārīkha al-zīārati 12 / 3 / 2021m.

istirjā'u 1277 ḥisāba barydi 'ilikturwniyyi li'a'ashkhāṣa tuqaddimū bibalāghāti 'abri manaṣṣati ecrime lishurṭata dubbī unẓur https:// www. albayan. ae / across- the- uae / news- and- reports / 2020- 05- 16- 1. 3561505 tārīkhin al-taṣaffuḥa 9 / 3 / 2021m.

āfāqu alkhidmāti alḥukūmiyyati al-dhakiyyati fī al'ālami al'arabiyyi 2018). silslata buḥwthi alqimmati alḥukūmiyyati

tarkiyyun manā kāmilu 2019). alḥimāyata aljinā'iyyata liḥaqqa alkhuṣūṣiyyati fī jarā'imi al-taṣwīri wa-l-tasjīli bidūni idhan dirāsata muqāranatin dāru al-nahḍati al'arabiyyati

taqryru alḥālati al-raqmiyyati li'āma 2020 " al'imārāti al'awlā 'ālamyā fī 6 qiṭā'ātin raqmiyyatin 'āmmin 2019" ،https:// www. albayan. ae / economy / local- market / 2020- 09- 03- 1. 3765863 tārīkha al-taṣaffuḥi 9 / 3 / 2021m.

ḥujjāziyyun 'abda alfattāḥi 2004). alḥukūmata al'ilikturwniyyata waniẓāmahā alqānūniyya dāru alfikri aljāmi'iyyi

ilḥasīnī 'ummāra 'ubbāsa 2017). jarā'ima alḥāswbi wa-l-'intrnt manshūrātu zayni alḥuqūqiyyati

ḥaṭṭābun ḥassiyanna 'aliyya muḥammada 2017). alḥimāyata aljazā'iyyata lil-baryda al'ilikturwniyya – dirāsata muqāranati risālata mājistīrin jāmi'ata alqādisiyyati https:// doi. org / 10. 37138 / 1425- 032- 001- 016

ḥammūdatun 'uliya maḥmūdu 2019). alwajīza fī al'a'aḥkāmi al'āmmati liqānūna al'uqūbāti alittiḥādiyya al-naẓariyyata al'āmmata lil-jazā'a aljinā'iyya akādīmiyytu shurṭati dubbiyyi

al-zu'biyyu jalāala wa-l-mnā'sa a'asāmmata 2010). jarā'ima tiqniyyati naẓmi alma'lūmāti al'ilikturwniyyati dāru al-thaqāfati lil-nashra

ṣāliḥun 'abīda 2015). sīāsata almusharri'i al-'imārāty limūājahata aljarā'imi al'ilikturwniyyati majallatu alfikri al-shurṭiyyi markaza buḥwthi al-shurṭati 95).

al-ṣaghīru jamīla 'abdi albāqī 2002). al-'intrnt wa-l-qānūna aljinā'iyya dāru al-nahḍati al'arabiyyati

ṭh maḥmūdun a'aḥamida 2018). al-tanaṣṣuta wa-l-talaṣṣuṣa 'alā sirriyyati alittiṣālāti al-shakhṣiyyati bayna al-tajrīmi wa-l-mashrū'iyyati dāru alfikri wa-l-qānūni

'abdu al'āṭī muḥammada al-sayyidi 2001). al-'intrnt wajawānibahā alqānūniyyata dāru al-nahḍati al'arabiyyati

'abdu alfattāḥi muḥammada al-sa'īdi 2020). alwajīza fī sharḥi qānūni al'uqūbāti alittiḥādiyya lidawlata al'imārāti ṭ al{fāqa almushriqata

al'uryāni muḥammada 'allī 2013). aljarā'ima alma'lūmātiyyata dāru aljāmi'ati lil-nashra https://

doi. org / 10. 21608 / mbse. 2013. 144722

'aṭā Allāhu 'imāma ḥusnayni khalīla 2016). alḥimāyata aljinā'iyyata liwasā'ila tiqniyyati alma'lūmāti fī al-tashrī'āti al'arabiyyati al'imārāti namūdhajan markaza al-dirāsāti wa-l-istiṭlā'āti wizārata al-dākhiliyyati

al'iwaḍiyyu 'abda alhādī 2005). aljawāniba alqānūniyyata lil-baryda al'ilikturwniyya dāru al-nahḍati al'arabiyyati

alqāsimiyyu 'ibrāhym muḥammada 2018). jarā'ima al-dukhūli wa-l-baqā'i ghayra almashrū'i fī niẓāmi almu'ālajati al{liyyati lil-mu'ṭayāti al'ilikturwniyyati fī al-tashrī'i al-'imārāty risālata mājistīrin jāmi'ata al'imārāti

mubādaratu ḥukūmati al'imārāti al-dhakiyyati https:// u. ae / ar- ae / about- the- uae / digital- uae / uae- mgovernment- initiative tārīkha al-taṣaffuḥi 10 / 3 / 2021m.

muḥammadun maḥmūda 'abdi al-Raḥmāni 2006). niṭāqa alḥaqqi fī alḥayāti alkhāṣṣata – dirāsatan fī alqānūni alwaḍ'iyyi wa-l-sharī'ati al'islāmiyyati dāru al-nahḍati al'arabiyyati

al-mwāfy 'abda al-rāziqi 2016). sharaḥa qānūnu mukāfaḥati jarā'imi tiqniyyati alma'lūmāti al-'imārāty alkitāba al'a'awwala ma'hadu dubbiyyu alqaḍā'iyyi

mūsan ḥawrā'a 2018). aljarā'ima almurtakibata 'abiru wasā'ilu al-tawāṣuli alijtimā'iyyi dirāsata muqāranatin dāru al-nahḍati al'arabiyyati

almawqi'u al'ilikturwniyyu libawwābata ḥukūmati al'imārāti https:// u. ae / ar- ae / about- the- uae / science- and- technology / key- sectors- in- science- and- technology / information- and- communication- technology tārīkha al-zīārati 12 / 3 / 2021m.

almawqi'u al'ilikturwniyyu ll'ajnda alwaṭaniyyata liru'uyata al'imārāti www. vision2021. ae tārīkha al-zīārati 11 / 3 / 2021m.

almawqi'u al'ilikturwniyyu lihay'iata tanẓīmi alittiṣālāti fī dawlati al'imārāti https:// www. tra. gov. ae / ar / about- tra / information- and- egovernment- sector. aspx tārīkha al-taṣaffuḥi 10 / 3 / 2021m.

almawsū'atu alḥurrata al'ālamiyyata lil-ma'lūmāti īkybydyā ar. wikipedia. org / wiki – tārīkha al-zīārati 7 / 3 / 2021m.

al-ymāḥy 'abdāllaha 2014). ijrā'āti taftīshi naẓmi alḥāsibi al{liyyi risālata mājistīrin akādīmiyyta shurṭati dubbiyyi

The Crime of Destroying the Contents of E-Mail in the UAE Law

Musab Abdalla Alnaqbi[1]
Khalid Muhammad Daqani[2]

Abstract:

This research aims to define the concept of e-mail, its legal nature, and the justifications for its protection. It also seeks to determine the legal structure for the crime of destroying the contents of e-mail, and to clarify the extent to which the UAE legislature addresses the substantive aspects related to protecting e-mail against the destruction of its contents using modern programs and technologies. The importance of this study lies in the fact that it captures the legal structure of the crime of destroying the contents of e-mail in the UAE legislation. It is conducted at a time witnessing the prevalence, multiplicity and diversity of data and information media and technologies and the reliance of individuals and government institutions on them in their daily activities. To this are added the consequent expansion and increase of crimes violating privacy through illegal access to e-mail and the risks threatening government data and information, as well as confidential mails among financial, commercial and economic institutions in the country. The research has reached several results, the most important of which is that the Emirati legislator did not specify the forms of attack on e-mail. In fact, the forms of attacks vary, and they occur when an offensive act is intentionally committed by the perpetrator. The destruction of the contents of e-mail occurs as a result of any conduct that causes destruction.

(1) College of Law - University of Sharjah (Sharjah - U.A.E.)
malnaour@gmail.com

(2) College of Law - University of Sharjah (Sharjah - U.A.E.)

These forms include the use of harmful and destructive codes and disruptive viruses that are transmitted from one computer to another and from one mail to another. They also include any other means that leads to the same end, as long as the legislator did not specify the forms of conduct that cause the crime of destroying the contents of an email and did not specify the results, either.

Keywords: e-mail, information destruction, UAE legislation, protected interest.