المجلة العراقية للبحوث الإنسانية والإجتماعية والعلمية
Iraqi Journal of Humanitarian, Social and Scientific Research
Print ISSN 2710-0952 Electronic ISSN 2790-1254
العـــدد 17A أيـار 2025
No.17A May 2025

# الحماية الجنائية الاحترازية من جرائم نظم الاتصالات الالكترونية – دراسة مقارنة

الباحث. عبد المحسن ميري محسن أ.م.د. ضياء عبد مسلم الغيبي
كلية القانون/ جامعة الكوفة
Abdulmohsenm.altayar@student.uokufa.edu.iq
dhiaam.alghaibi@uokufa.edu.iq

**الملخص:**

برزت الحماية الجنائية الاحترازية كوسيلة أساسية لمكافحة جرائم نظم الاتصالات الالكترونية قبل وقوعها، وذلك من خلال تجريم الأفعال التي تهدد أمن البيانات والنظم المعلوماتية. ومنع الأدوات والتقنيات التي تُستخدم في تنفيذ هذه الجرائم. وقد تبنّت الحماية الاحترازية التشريعات في مصر، فرنسا، الإمارات، والجزائر لحماية نظم الاتصالات الإلكترونية انسجاما مع الاتفاقيات الدولية، من خلال تجريم حيازة أو تداول الأدوات والتقنيات المستخدمة في ارتكاب الجرائم الإلكترونية، وتجريم إنشاء المواقع أو الحسابات الإلكترونية بقصد تسهيل أو تنفيذ هذه الجرائم، فضلا عن إجراءات الحماية الاحترازية من هذه الجرائم قبل وقوعها.

الكلمات المفتاحية: (الحماية الجنائية، جرائم نظم الاتصالات الالكترونية).

# Precautionary Criminal Protection Against Electronic Communications Systems Crimes – A Comparative Study

**Researcher: Abdul Mohsen Miri Mohsen, Assistant Professor: Dhiaa Abdul Muslim Al-Ghaibi**
**College of Law, University of Kufa**
**Abdulmohsenm.altayar@student.uokufa.edu.iq**
**dhiaam.alghaibi@uokufa.edu.iq**

## Abstract

Precautionary criminal protection has emerged as a basic means of combating electronic communications system crimes before they occur, by criminalizing acts that threaten the

security of data and information systems, and preventing the tools and technologies used to carry out these crimes. Precautionary protection has been adopted by legislation in Egypt, France, the UAE, and Algeria to protect electronic communications systems in line with international agreements, including by criminalizing the possession or circulation of tools and technologies used to commit electronic crimes, and criminalizing the creation of websites or electronic accounts with the intent to facilitate or carry out these crimes, in addition to precautionary protection measures against these crimes before they occur.
Keywords: (criminal protection, electronic communications systems crimes).

أولاً: موضوع البحث:

أصبحت نظم الاتصالات الإلكترونية اليوم حجر الأساس في الحياة الرقمية، حيث تُستخدم في مختلف المجالات الشخصية والمؤسسية، مما يجعلها هدفًا رئيسيًا للجرائم الإلكترونية. ونظرًا لخطورة هذه الجرائم وتأثيرها على الأمن السيبراني، برزت الحماية الجنائية الاحترازية كوسيلة أساسية لمكافحتها قبل وقوعها، وذلك من خلال تجريم الأفعال التي تهدد أمن البيانات والنظم المعلوماتية. ومنع الأدوات والتقنيات التي تُستخدم في تنفيذ هذه الجرائم.

كما أولت التشريعات في الدول المقارنة اهتمامًا بالحماية الوقائية، من خلال تجريم حيازة أو تداول الأدوات والتقنيات المستخدمة في ارتكاب الجرائم الإلكترونية، وتجريم إنشاء المواقع أو الحسابات الإلكترونية بقصد تسهيل أو تنفيذ هذه الجرائم، ورغم هذه التطورات التشريعية في الدول المقارنة، لا يزال التشريع العراقي يعتمد على نصوص قانون العقوبات التقليدية التي لم تُصمم لمواجهة الجرائم الإلكترونية المعقدة

ثانياً: أهمية البحث:

تزداد أهمية دراسة موضوع الحماية الجنائية الاحترازية من جرائم نظم الاتصالات الالكترونية بسبب ازدياد استخدام نظم الاتصالات الالكترونية المستمر، وتنوع استخدام وسائل الاتصالات الالكترونية في جميع نواحي الحياة في ظل التقدم التكنلوجي للاتصالات، وظهور أساليب إجرامية

جديدة تصاحب هذا التطور التكنلوجي، الذي لم يعالجها المشرع العراقي لذا تطلب تقديم دراسة لحماية المجتمع، من خلال توفير الحماية الجنائية الاحترازية من جرائم نظم الاتصالات الالكترونية.

ثالثاً: مشكلة البحث:

تتمثل المشكلة في مدى كفاءة القوانين الوطنية في الدول محل الدراسة في تأسيس حماية جنائية احترازية من جرائم نظم الاتصالات الالكترونية مقارنة بالمعايير والالتزامات الدولية، وماهي أوجه القوة والقصور في هذه التشريعات وخاصة في العراق في إطار القواعد الموضوعية والقواعد الإجرائية؟

رابعاً: أهداف البحث:

اهداف الدراسة هو تحديد مفهوم الحماية الاحترازية والوقوف على الحماية الجنائية الاحترازية من جرائم نظم الاتصالات الالكترونية لمنع هذه الجرائم من خلال تناول قوانين الدول المقارنة والاتفاقية العربية لمكافحة الجرائم الالكترونية لسنة ٢٠١٠ واتفاقية بودابست لسنة ٢٠٠١ بهذا الشأن وتحليلها، واوجه القصور في النصوص القانونية التي لم يعالجها المشرع العراقي في قانون العقوبات العراقي وقانون أصول المحاكمات الجزائية.

خامساً: نطاق البحث:

ان نطاق دراستنا هو بيان القواعد الموضوعية ة الخاصة بمنع جرائم نظم الاتصالات الالكترونية وخاصةً المذكورة في قانون الفرنسي والجزائري والمصري والإماراتي وقانون العقوبات رقم ١١١ لسنة ١٩٦٩ المعدل وكذلك مشروع قانون مكافحة الجرائم الالكترونية لعام ٢٠١٩ والذي لم يقر لحد الان وكذلك الاتفاقية العربية لمكافحة الجرائم الالكترونية لسنة ٢٠١٠ واتفاقية بودابست لسنة ٢٠٠١ بخصوص مكافحة الجرائم الالكترونية.

سادساً: منهج البحث:

منهج الدراسة سوف يعتمد المنهج الاستقرائي والتحليلي المقارن عن طريق تحليل النصوص القانونية الخاصة في جرائم نظم الاتصالات الالكترونية ومقارنتها مع بعضها البعض وخاصة فيما يتعلق بالدول المقارنة، وهي القانون المصري والفرنسي والجزائري والاماراتي والعراقي وكذلك الاتفاقية

العربية لمكافحة الجرائم الالكترونية لسنة ٢٠١٠ واتفاقية بودابست لسنة ٢٠٠١ فيما يتعلق بالقواعد الموضوعية الاحترازية.

ثامناً: خطة البحث:

سنعالج هذا الموضوع من خلال خطة تتضمن مقدمة ومطلبين نعرض في المطلب الأول أركان جريمة أنشاء الحسابات الوهمية، اما المطلب الثاني نعرض فيه الإحكام الإجرائية الخاصة بإنشاء الحسابات الوهمية وتأثير في الرأي العام اما الخاتمة ستضمنها أهم النتائج التي تم التوصل إليها، مع تعزيزها بالمقترحات التي.

## المطلب الأول

## التعريف بتجريم حيازة الأجهزة والمعدات الخاصة لارتكاب جرائم نظم الاتصالات الالكترونية

من اجل معرفة المقصود من التعريف بالتجريم سنتناول طبيعة جريمة حيازة الأجهزة والمعدات والآلات الخاصة لارتكاب جرائم نظم الاتصالات الالكترونية سنتناول موضوع الجريمة واهم أدوات ارتكابها وتحليلها والتعرف على محل الجريمة.

**١- موضوع التجريم:**

موضوع التجريم حسب ما نصت عليه التشريعات في الدول محل المقارنة في تجريم الحيازة حيث نص المشرع المصري في المادة ٢٢ من قانون مكافحة جرائم تقنية المعلومات " كل من حاز او أحرز او جلب او باع او أتاح او صنع او أنتج او استورد او صدر او تداول"[١]، اما المشرع الفرنسي في المادة (٢٢٦-٣) المعدلة بموجب قانون رقم ٩٣٦-٢٠٢٠ المؤرخ في ٣٠ يوليو ٢٠٢٠ في الفقرة (١) التي نصت " تصنيع او استيراد او حيازة او عرض او تأجير او بيع اجهزة تقنية قادرة على تنفيذ الأفعال التي تشكل جريمة ...." [٢]، اما المشرع الاماراتي في المادة (١٤) من قانون مكافحة جرائم تقنية المعلومات المعدل لقت نصت على ".... كل من حصل على رقم سري او شفرة او كلمة مرور او أي وسيلة أخرى للدخول الى وسيلة تقنية معلومات او موقع الكتروني، او نظام معلومات الكتروني، او شبكة معلوماتية، او الكترونية. ..... كل من اعد او صمم او انتج او باع

او اشترى او استورد او عرض للبيع او أتاح أي برامج معلوماتي او وسيلة تقنية معلومات ، او روج باي طريقة روابط لمواقع الكترونية او برامج معلوماتي، او أي وسيلة تقنية معلومات مصممة لأغراض ارتكاب او تسهيل او تحريض على ارتكاب الجرائم المنصوص عليها في هذا المرسوم بقانون" [٣] ، اما المشرع الجزائري في المادة ٣٩٤ مكرر ٢ من قانون العقوبات في القسم السابع مكرر الخاص بالمساس بأنظمة المعالجة الالية للمعطيات حيث نصت " ١- تصميم او بحث او تجميع او توفير او نشر او الاتجار في معطيات مخزنة او معالجة او مراسلة عن طريق منظومة معلوماتية يمكن ان ترتكب بها الجرائم المنصوص عليها في هذا القسم. ٢- حيازة او افشاء او نشر او استعمال لاي غرض كان المعطيات المتحصل عليها من احدى الجرائم المنصوص عليها في هذا القسم." [٤] .

نرى ان المشرع المصري استعمل مصطلحات (حاز او أحرز او جلب او باع او أتاح او صنع او أنتج او استورد او صدر او تداول)، اما المشرع الفرنسي استعمل مصطلحات (استيراد او حيازة او عرض او تأجير او بيع)، اما المشرع الاماراتي استعمل المصطلحات (اعد او صمم او أنتج او باع او اشترى او استورد او عرض للبيع او أتاح)، اما المشرع الجزائري استعمل (حيازة او افشاء او نشر او استعمال).

تتكون نظم الاتصالات الالكترونية من أجهزة ومعدات والآلات وتكون هذه المواد هي مواد مادية ملموسة ، وكذلك تتكون من أشياء غير ملموسة (معنوية) ، الأشياء المادية لنظم الاتصالات الالكترونية مثل الأجهزة والسيرفرات والمعدات وأدوات التخزين ، اما الأدوات والمعدات الغير ملموسة تتمثل بالبرامج المصممة وأنظمة التشغيل والاكواد (كلمات المرور) والشفرات والرموز والبيانات وان هذه الأدوات هي متممات عمل الاتصالات الالكترونية من خلال الهواتف الذكية والحواسيب الالي ، حيث تجتمع المواد المادية والغير مادية بأسلوب تقني وهندستها الكترونيا لتخزين ومعالجة البيانات عن طريق وحدة الادخال (input unit) و، وحدة المعالجة (Processing Unit) ويتم نقلها عبر السيرفرات (Computer Servers) والشبكات (networks) ، التي تربط الحواسيب أو الهواتف الذكية مع بعضها عن بعد ، حيث تقوم بهذه المهام السيرفرات كبيرة تابعة لشركة الاتصالات ، كما

توفر هذه السيرفرات التعب والجهد للعملاء من خلال تخزين البيانات في ملفات ووسائط متعددة ، وكذلك تخزين بيانات الاتصالات في ذاكرة (Ram) والقرص صلب (hard drive disk)، ولما القانون جرم بعض الصور التي تقع باستخدام تلك الوسائل والمعدات المادية والمعنوية كان من الطبيعي للمشرع ان يجرم الأدوات التي تستخدم في ارتكاب جرائم نظم الاتصالات الالكترونية . [٥]

اما بخصوص محل الجريمة هو الاداة او الوسيلة التي ممكن ان تستخدم في ارتكاب أي من الجرائم نظم الاتصالات الالكترونية المنصوص عليها في القانون، أي ان الفعل المتمثل بالحيازة او البيع او الاحراز او التداول وغيرها للأجهزة او الآلات او المعدات او البرامج والأكواد والشفرات التي تستخدم كأداة للجريمة. [٦]

نود الإشارة الى ان المقصود بالأجهزة هي الأجهزة التي يمكن استخدامها لارتكاب الجريمة، أيا كان نوع هذه الأجهزة او طريقة عملها يمكن استخدامها في ارتكاب جرائم الاتصالات الالكترونية او جرائم نظم المعلوماتية المذكورة في القانون ، اما البرامج هي البرامج المخصصة لاستخدام غير المشروع سواء كانت برامج جاهزة او برامج مطورة او مصممة من قبل الجاني، كما تعرف البرامج المعلوماتية بانها مجموعة الأوامر والتعليمات المعبر عنها بأية لغة او رمز او إشارة تحقق إعطاء الايعاز للحاسب الالي ، والتي تتخذ أي شكل من الاشكال ويمكن استخدامها بطريق مباشر او طريق غير مباشر في حاسب آلي لأداء وظيفة معينة تحقيق نتيجة سواء كانت هذه الأوامر والتعليمات في شكلها الأصلي او في أي شكل اخر تظهر فيه من خلال حاسب آلي او نظام معلوماتي .

ان الوسيلة التي تستخدم في ارتكاب جرائم نظم الاتصالات بحسب ما نص عليها المشرع في الدول محل المقارنة وهي:

**أ- الأجهزة او المعدات والآلات**

المقصود بالأجهزة هي الأدوات التي تؤدي عملا ما مثل جهاز الهاتف او جهاز الاستقبال او جهاز الارسال او الحاسب الالي او أي أداة أخرى ممكن ان تقوم بأرسال الرسائل او استقبالها او

تقوم بتامين اتصال عن طريق المحادثة كما هناك أجهزة لها القابلية على تغيير بيانات النظم وإعادة برمجتها ، اما المعدات هي العدد والتجهيزات فممكن اعتبار الحاسب الالي من الأجهزة وهو كذلك من المعدات حيث يمكن استعماله في تامين الاتصال بشبكة المعلومات وكذلك اعداد البيانات ونظم المعلومات وكذلك بالنسبة الى الهواتف الذكية الحديثة والآيباد وغيرها من الأجهزة التي تحقق الدخول الى شبكات المعلومات وشبكة الانترنت. (٧)

**ب-البرامج واكواد المرور**

ان المقصود بالبرامج اصطلاحا هي سلسلة من الإجراءات او العمليات الحسابية المعقدة تجري برموز واشارات وأرقام داخل الحاسب الالي لحل مسالة معينة، أي انه هو مجموعة من الأوامر والتعليمات تبين للحاسب الالي تسلسل الخطوات التي يجب القيام بها في أداء مهام معينة لحل المشكلة التي تم إدخالها واستخراج النتائج، ويتم تخزين البرنامج في الذاكرة الرئيسية للحاسب الالي (Computer main memory) لتوجيهه لإنجاز العمليات المطلوبة وفق المعطيات وتمكنه أيضا من إدارة ومراقبة وتنظيم مكوناته لتحقيق مهامه. (٨)

اما الاكواد ويقصد بها الأوامر والتعليمات المكتوبة بلغة من لغات البرمجة التي تتمثل بأرقام ورموز وحروف خاصة بلغة الحاسوب التي تعتبر مفتاح من اجل بدء العمل وفق الاوامر المكتوبة التي تم تصميم البرنامج فيها لقيام الحاسب الالي بمعالجته وإعطاء النتائج من خلاله وهي طريقة من طرق الحماية للبيانات والحواسيب. (٩)

**ت-الشفرات**

المقصود بالتشفير هو استخدام الأرقام والرموز وفق طريقة معينة باستخدام معادلات رياضية لا يمكن قراءتها وفق ما تم برمجة الحاسوب عليها حيث يتم من خلالها حفظ امن وسرية المعلومات، وفك التشفير هو كسر للرموز المؤمنة وخرق الاتصالات الامنة، أي ان التشفير هو عملية تحويل المعلومات الى شفرات غير مفهومة لمنع الأشخاص غير المرخصين من الاطلاع على المعلومات او

يمنعهم من فهمها ، كما تمكن تكنولوجيا التشفير الرقمي الذي يقوم به الجناة من حماية المحتوى المتبادل بطريقة خاصة تجعل من المستحيل على السلطات المسؤولة على تطبيق القانون النفاذ الى ذلك المحتوى، فاذا قام المجرم بتشفير الرقمي للمحتوى الذي ينقله من خلال اختراقه موقع او حساب خاص فان السلطات ليس باستطاعتها سوى اعتراض اتصال المشفر الذي يقيمه المجرم ، دون إمكانية السلطات من تحليل المحتوى، وبدون النفاذ الى المفتاح التشفير المستعمل في تشفير الملفات الذي ينقلها المجرم ، فان إمكانية إزالة التشفير من قبل السلطات قد تستغرق وقتا طويلا جدا وقد تفشل عملية فك التشفير. (١٠)

بعد التعرف على المصطلحات المستخدمة في النصوص التشريعية في الدول المقارنة يتبين لنا ان الجريمة تتخذ كافة صور الافعال الإيجابية التي يتكون منها الركن المادي لها ، المتمثلة بحيازة او احراز او جلب او بيع او التداول او استيراد او تصدير وغيرها للأجهزة والآلات والمعدات والبرامج والاكواد والشفرات التي تستخدم لارتكاب الجريمة ، وبغير تصريح من الجهة المختصة بتنظيم الاتصالات او بدون مسوغ من الواقع او من القانون، ان جميع هذه الافعال تمثل أفعال إيجابية ولكنها ليست متشابهة من حيث الاستمرارية، أي كونها جريمة مستمرة او جريمة وقتية، حيث ان الحيازة والاتاحة والاحراز تمثل جميعها جريمة مستمرة ، وان الاحراز او الحيازة او الاتاحة تتحقق باستمرارية القيام العمل، اما الجريمة في صورة البيع او الجلب او الاستيراد او التصنيع او الإنتاج او التداول الأجهزة والآلات الخاصة بارتكاب الجريمة، فهذه الأفعال وقتية ، يتحقق الاعتداء بمجرد حدوثه دون الحاجة الى الاستمرارية ، وهذا يعني ان الجريمة تقع كاملة مجرد حدوثه دون الحاجة الى الاستمرارية ، أي تقع بمجرد البيع او التصنيع او الإنتاج او التداول ، ومن جانب اخر تعتبر الجريمة بكافة صورها التي تطرقنا لها في الحالتين سواء كانت مستمرة او وقتية من جرائم الخطر وليس جرائم الضرر. (١١)

ان المشرع في دول المقارنة لم يشترط الضرر الفعلي على المجني عليه ، ولكن يتطلب لوقوع الجريمة هو الحيازة او تداول او اتاحة البيع او وغيرها من الأفعال التي ذكرناها لغرض استخدامها في ارتكاب الجريمة من جرائم نظم الاتصالات الالكترونية او جرائم تقنية المعلومات، على اعتبار ان

هذه الأفعال المتمثلة بحيازة الأجهزة او المعدات او تصنيعها هو في حد ذاته خطر يهدد الاتصالات الالكترونية او تقنية المعلومات وبغض النظر عن استخدامها في الجريمة او عدم استخدامها المهم في تحقق الجريمة هو توفر أي صورة من الصور التي تم ذكرها لذلك ان هذه الصور هي جميعها جرائم خطر ، لذلك ان هذه الجريمة من الجرائم الشكلية أي انها تقع تكتمل بمجرد وقوع الفعل المكون لها دون ان يتطلب المشرع في حصولها أي تنجية إجرامية تترتب على الفعل [١٢] ، لذلك اتجه المشرع في الدولة المقارنة الى تجريم هذه الأفعال من اجل الحماية الجنائية الاحترازية لمنع وقوعها.

**٢- موقف التشريعي للدول من التجريم:**

بالنسبة الى المشرع المصري لقد جرم في المادة ٢٢ من قانون رقم ١٧٥ لسنة ٢٠١٧ حيازة وجلب وصناعة معدات او أجهزة او برامج لاستخدامها في ارتكاب جرائم تقنية المعلومات بأنواعها المنصوص عليها في القانون حيث نصت المادة "يعاقب بالحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن ثلاثمائة الف جنيه ولا تجاوز خمسمائة الف جنيه او بإحدى هاتين العقوبتين ، كل من حاز او احرز او جلب او باع او أتاح او صنع او انتج او استورد او صدر او تداول باي صورة من صور التداول ، أي أجهزة او معدات او أدوات او برامج مصممه او مطورة او محورة او اكواد مرور او شفرات او رموز او أي بيانات مماثلة بدون تصريح من الجهاز او مسوغ من الواقع او القانون ،وثبت ان ذلك السلوك كان بغرض استخدام أي منها في ارتكاب او تسهيل ارتكاب أي جريمة من جرائم المنصوص عليها في هذا القانون ، او إخفاء اثار او ادلتها او ثبت ذلك الاستخدام او التسهيل او الاخفاء". [١٣]

ان ما اتجه اليه المشرع المصري في نص المادة (٢٢) هو تطبيقا لحكم المادة التاسعة من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات سابقة الذكر. [١٤]

نرى من خلال المادة ٢٢ ان المشرع المصري قد استبق وقوع الجريمة حيث عاقب على الأفعال التي تؤدي الى ارتكاب الجريمة من خلال معاقبة كل من الصنع او حاز او أحرز او جلب او باع او أتاح او صنع او أنتج او استورد او صدر او تداول باي صورة من صور التداول وبذلك

وضع هذا النص كحماية جنائية احترازية من اجل منع وقوع الجريمة وذلك لخطورتها على أنظمة الاتصالات والأنظمة المعلوماتية سواء كانت تعود للدولة او للأشخاص وانتهاك حرمتها وسريتها، كما ان المشرع المصري في هذا النص استخدم كثير من المصطلحات متشابهة ، كان من الاجدر ان يختصر هذه المصطلحات بعبارات تدل على تجريم تصنيع او استيراد او حيازة او تداول الأجهزة او الآلات والمعدات او البرامج التقنية المعلومات التي تستخدم في جرائم نظم الاتصالات الالكترونية او تقنية المعلومات بشكل غير مشروع ،كما اسهب المشرع المصري في استخدام البرامج مصممة او مطورة او محورة او اكواد مرور او شفرات او رموز او أي بيانات مماثلة نرى ممكن اختصارها باستخدام برامج مصممة تستخدم في الجريمة حيث ان جميع المصطلحات التي استخدمها المشرع المصري من محورة او اكواد او شفرات او رموز فهي برامج تستخدم في الاختراق نظم المعلوماتية ونظم الاتصالات الالكترونية فهي تعتبر أداة للارتكاب الجريمة.

بخصوص المشرع الفرنسي قد نص على مجموعة من الأفعال تصب جميعها بالتعامل في الاجهزة صالحة لان تُرتكب بها احدى الجرائم التي تمس نظم الاتصالات الالكترونية ، وتنتهك سرية البيانات والمعلومات او سلامتها او اتاحتها ووفرتها بشكل غير مشروع، وذلك بموجب المادة (٢٢٦-٣) المعدلة بقانون عدد ٩٣٦ لسنة ٢٠٢٠ والتي نصت "يعاقب على ما يلي بالسجن لمدة خمس سنوات وغرامة قدرها ٣٠٠ الف يورو:١- تصنيع او استيراد او حيازة او عرض او تأجير او بيع الأجهزة التقنية او الأجهزة ذات الطبيعة التي تسمح بتنفيذ العمليات التي تشكل الجريمة المنصوص عليها في المادة (٢٢٦-١٥) او التي تهدف الى الكشف عن المحادثات عن بعد، مما يجعل من الممكن تنفيذ الجريمة المنصوص عليها في المادة (٢٢٦-١) او ان يكون هدفها التقاط بيانات الكمبيوتر المنصوص عليها في المواد(٧٠١-١٠٢) من قانون الإجراءات الجنائية وقانون رقم (٨٥٣-٢) من قانون الامن الداخلي والواردة في قائمة توضع وفقا للشروط المنصوص عليها في مرسوم نفسه او دون الامتثال للشروط التي يحددها هذا الترخيص".[١٥]

كما ذهب المشرع الفرنسي الى ابعد من ذلك ، حيث نص في الفقرة الثانية من نفس المادة بالعقوبة على الترويج عنها والاعلان لصالح جهاز تقني يحتمل ان يسمح بارتكاب الجرائم المنصوص عليها في القانون ، حيث نص في الفقرة الثانية من نفس المادة على "القيام بالإعلان لصالح جهاز او جهاز تقني من شانه ان يسمح بارتكاب الجرائم المنصوص عليها في المادة (٢٢٦-١) والفقرة الثانية من المادة (٢٢٦-١٥) عندما يشكل هذا الإعلان تحريضاً على ارتكاب هذه الجريمة ، او يكون هدفه الاستيلاء على البيانات الحاسوبية المنصوص عليها في المواد (٧٠٦-١٠٢-١) من قانون الإجراءات الجنائية و المادة (L.٢-٨٥٣ ) من قانون الامن الداخلي ، عندما يشكل هذا الإعلان تحريضا على الاستخدام الاحتيالي له". (١٦)

نرى ان المشرع الفرنسي قد جرم حيازة او تداول أجهزة تقنية المعلومات التي يمكن استخدامها بتنفيذ العمليات التي تشكل جريمة المنصوص عليها في القانون وكذلك ذهب المشرع الفرنسي الى ابعد من الحيازة حيث جرم الإعلان والترويج الى الأجهزة التي ممكن ان تستخدم في ارتكاب الجريمة وحيث يعتبر هذا النص هو حماية جنائية احترازية لمنع جرائم نظم الاتصالات الالكترونية في هذا النص.

اما المشرع الأمارتي جرم الحيازة في المادة (١٦) من قانون رقم (٣٤) لسنة ٢٠٢١ نصت على " يعاقب بالحبس مدة لا تقل عن (٢) سنتين والغرامة التي لا تقل عن مائتي ألف درهم ولا تزيد على مليون درهم أو بإحدى هاتين العقوبتين كل من حاز، او أحرز او اعد او صمم او أنتج او استورد او أتاح او استخدم أي برامج معلوماتي او وسيلة تقنية معلومات او اكواد مرور او رموز او استخدم التشفير بقصد ارتكاب أي جريمة المنصوص عليها في هذا المرسوم بقانون او اخفى ادلتها او اثارها او الحيلولة دون اكتشافها". (١٧)

نرى ان المشرع الاماراتي في هذا النص لم يتطرق الى الأجهزة او المعدات او الآلات التي تعتبر من الاشياء المادية التي تستخدم في ارتكاب الجريمة بل عاقب اعداد او التصميم او أنتاج او البيع او الشراء او الاستيراد او العرض للبيع او الإتاحة للجمهور أي برنامج معلوماتي، وهذا يعني ان المشرع الاماراتي قد جرم التعامل بالأشياء المعنوية التي يمكن استخدامها في ارتكاب جريمة

الاتصالات الالكترونية او تقنية المعلومات ، فيعاقب الجاني على السلوك وحتى لو لم يتحقق الغرض منها فالمشرع قصد من هذا النص حماية جنائية احترازية لمنع وقوع الجريمة، من خلال النص لأغراض ارتكاب الجريمة او تسهيل او تحريض على ارتكاب الجرائم المنصوص عليها ، ولو ان المشرع اشترط وقوع الجريمة نكون بذلك امام احكام المشاركة الاجرامية [١٨].

وكذلك نرى ان المشرع الأمارتي لم يتطرق الى التعامل بالأجهزة التي تستخدم في ارتكاب جريمة تقنية المعلومات والتي تعتبر من الأشياء المادية، كما فعل المشرع الفرنسي والمشرع المصري اكتفى بالأشياء المعنوية بالبرامج المعلوماتية او أي وسيلة تقنية معلومات بموجب المادة (١٦) من قانون مكافحة جرائم تقنية المعلومات.

ونرى ان من الاجدر على المشرع الاماراتي الأشياء المادية والمعنوية وان يذكر الأجهزة والمعدات والآلات التي يمكن ان تستخدم في ارتكاب الجريمة.

اما المشرع الجزائري لقد عالج هذه الجريمة في الفقرة الثانية من المادة ٣٩٤ مكرر ٢ من قانون رقم (٦٦-١٥٦) المعدل في القسم السابع المكرر الخاص بالمساس بأنظمة المعالجة الالية للمعطيات، التي نصت على "يعاقب بالحبس شهرين الى ثلاث سنوات وبغرامة من مليون دينار جزائري الى خمس ملايين دينار جزائري كل من يقوم عمدا وعن طريق الغش بما يلي: حيازة او افشاء او نشر او استعمال لأي غرض كان المعطيات المتحصل عليها من احدى الجرائم المنصوص عليها في هذا القسم." [١٩]

بموجب هذه المادة تتحقق هذه الجريمة بأحد الأفعال المتمثلة في حيازة معطيات متحصلة من احدى الجرائم التي ذكرها المشرع الجزائري كجريمة البقاء غير الصرح به وغيرها او افشائها أي نقلها الى الغير او نشرها عن طريق أي وسيلة من وسائل الاعلام او استعملها الجاني لاي غرض معين، كما لا يتطلب لتجريمها حدوث نتيجة فعلية، ولا يشترط تحقق ضرر فعلي يقع على معطيات او أنظمة معلوماتية بل تجرم أفعال خطرة يتحقق من خلالها الضرر الفعلي. [٢٠]

نرى من خلال المادة ٣٩٤ مكرر ٢ ان المشرع الجزائري جرم المشرع الجزائري حيازة او افشاء او نشر او استعمال لاي غرض كان، ولم يحدد الغرض المفروض ان يذكر الاتصالات الالكترونية التقنية المعلومات بالتحديد وكما حدد المعطيات المتحصلة عليها من احدى الجرائم المنصوص عليها في القانون.

ويثار تساؤل هل المعطيات التي لم يتم الحصول عليها من الجرائم المذكورة غير مشمولة في هذا القانون؟

ومن خلال النص يتبين ان المشرع الجزائري جرم التعامل بالمعلومات سواء بإفشائها او نشرها او استعملها وبذلك يكون المشرع الجزائري انتهج نهج المشرع الأمارتي.

ان الاتفاقية بودابست قد اشارت على ان جرائم الاعتداء على نظم المعالجة الالية يتطلب لارتكابها حيازة وسائل الاختراق او الولوج كأدوات القرصنة او أي أدوات أخرى، وان هناك دافعاً قويا للحصول على هذه الوسائل التي تستخدم لأغراض إجرامية، مما قد يؤدي الى خلق نوع من المتاجرة والسوق السوداء لأنتاج وتوزيع مثل هذه الأدوات، وتضيف المذكرة التفسيرية "ومن اجل وقاية أكثر فاعلية من هذه المخاطر فانه يجب على قانون العقوبات ان يحظر الأفعال راجحة الخطورة من المنبع قبل ارتكاب الجرائم المشار اليها في المواد (٢ الى ٥) من الاتفاقية". [٢١]

كما نصت الاتفاقية بودابست في الفقرة الثانية من الماد (٦) على " تجريم الإنتاج او البيع او الشراء او الاستعمال او الاستيراد او التوزيع او الاتاحة بوسيلة أخرى لاي برنامج حاسوبي مصمم او معد خصيصا لغرض ارتكاب أي من جرائم المقررة في المواد (٢-٥) من هذه الاتفاقية. ويشير مصطلح التوزيع إلى الفعل النشط لنقل البيانات إلى الغير، بينما يحيل مصطلح إتاحة على توفير أجهزة عبر الإنترنت ليستخدمها الغير.

ويهدف هذا المصطلح أيضا إلى تغطية إنشاء أو تجميع وصلات تشعبية من أجل تيسير النفاذ إلى هذه الأجهزة. ويشير إدراج برنامج حاسوبي إلى البرامج المصممة على سبيل المثال من أجل تغيير أو حتى إتلاف البيانات أو التدخل في تشغيل الأنظمة، من قبيل برامج الفيروسات أو البرامج المصممة أو المكيفة للحصول على إمكانية النفاذ إلى أنظمة الكمبيوتر". [٢٢]

كما جرمت الاتفاقية في الفقرة (٥ و٦) من المادة (٦) حيازة الأجهزة او المواد المبينة في الفقرة (١) والفقرة (٢) من نفس المادة "بنية ارتكاب أي من الجرائم المنصوص عليها في المواد من (٢الى ٥) من الاتفاقية". [٢٣]

وكما نرى ان اتفاقية بودابست قيدت النطاق في ذلك المسلك بخصوص نوع الأجهزة موجب لمادة (٦) في فقرتها الثالثة حيث نصت على " ... قيدت الاتفاقية نطاقه في الحالات التي يتم فيها تصميم أو تكييف الأجهزة بشكل موضوعي أساسا لغرض ارتكاب جريمة. هذا وحده من شأنه أن يستبعد عادة الأجهزة ذات الاستخدام المزدوج" [٢٤]، منها وبالتالي فان هذا النص يستبعد عادة الأجهزة ذات الاستخدام المزدوج حسب نص المادة (٦) من الاتفاقية.

اما الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في المادة (٩)، جريمة إساءة استخدام وسائل تقنية المعلومات، في الفقرتين الأولى والثانية الى الجريمة حيث نصت على"١- انتاج او بيع او شراء او استيراد او توزيع او توفير: أ- اية أدوات او برامج مصممة او مكيفة لغايات ارتكاب الجرائم المبينة في المادة السادسة الى المادة الثامنة. ب- كلمة سر نظام معلومات او تشفير دخول او معلومات مشابهة يتم بواسطتها دخول نظام معلومات ما يقصد استخدامها لأية من الجرائم المبينة في المادة السادسة الى المادة الثامنة. ٢- حيازة اية أدوات او برامج مذكورة في الفقرتين أعلاه، بقصد استخدامها لغايات ارتكاب أي من الجرائم المذكورة في المادة السادسة الى المادة الثامنة." [٢٥]

ونرى ان الاتفاقية بودابست قد استبعدت الأجهزة ذات الاستخدام المزدوج حسب نص المادة (٦) من الاتفاقية، اما الاتفاقية العربية والمشرع في الدول المقارنة كالمشرع المصري او المشرع الفرنسي اتجه الى التجريم بشكل واسع في هذا المجال حيث ان الواقع يبين ان كثير من البرامج والمعدات والآلات الخاصة بتقنية المعلومات والتي تقوم بتصنيعها الشركات العالمية الكبرى في هذا المجال تستخدم في امن وحماية نظم المعلومات وحماية الشبكات من اجل الكشف عن الاختراقات، في نظم الحاسبات والهواتف الذكية، وكذلك يمكن استغلالها واستخدامها في جرائم نظم المعلوماتية ، لذا نرى من الاجدر على المشرع ان يحدد بشكل دقيق البرامج والآلات والمعدات والأجهزة التي يمكن اعتبار حيازتها او تداولها جريمة يعاقب عليها القانون.

اما بخصوص المشرع العراقي لم يعالج جريمة حيازة الأجهزة المعدات والآلات الخاصة بارتكاب جرائم نظم الاتصالات الالكترونية في قانون العقوبات رقم ١١١ لسنة ١٩٦٩ وبالإشارة الى مشروع قانون مكافحة الجرائم الالكترونية لسنة ٢٠١٩ كذلك لم يعالج جريمة حيازة المعدات والآلات الخاصة بارتكاب جرائم نظم الاتصالات الالكترونية ولم يورد نص بخصوص الحماية الجنائية الاحترازية لنظم الاتصالات الالكترونية.

وتجدر الإشارة الى ان الاعمال التحضرية التي تسبق حصول الجريمة هي غير معاقب عليها في القانون الا في حالة اذا كانت في حد ذاتها جريمة، اما الحيازة وجلب الأجهزة والبرمجيات التي تمكن من الدخول غير المشروع والاعتراض والاختراق وغيرها مجًرم في حد ذاته لخطورة هذه الأجهزة وكذلك لمنع ارتكاب الجريمة من جانب اخر، وان خطورة هذه الأجهزة تكمن في الاختراق وكذلك إخفاء مرتكب الجريمة لها وعدم القدرة على التعرف على المجرم والتحقق من هويته وكذلك العبث بالأدلة الرقمية التي تساعد القائمين بالتحقيق الوصول الى الحقيقة.[٢٦]

## الفرع الثاني

### التعريف بتجريم أنشاء او تصميم موقع او حساب لارتكاب جرائم نظم الاتصالات الالكترونية

من اجل معرفة ما المقصود بتجريم أنشاء او تصميم موقع او حساب لارتكاب جرائم نظم الاتصالات الالكترونية سنتناول موضوع التجريم وبعدها نتناول الموقف التشريعي من التجريم.

**١- موضوع التجريم**

من استقراء قوانين دول محل المقارنة يتحقق قيام الجريمة بعدة أفعال تكون الركن المادي لها، حيث ان المشرع المصري أشار الى فعل الانشاء او الإدارة او الاستخدام حساب خاص او موقع خاص بغرض ارتكاب جريمة من جرائم نظم الاتصالات الالكترونية، وجميعها صور إيجابية غير سلبية. [٢٧]

اما المشرع الاماراتي أشار الى انشاء او إدارة او اشراف على موقع الكتروني بقصد ارتكاب جرائم نظم الاتصالات الالكترونية ضمن قانون رقم (٣٤) لسنة ٢٠٢١ في شان مكافحة الشائعات وجرائم الالكترونية في المادة (١٧) وهي جريمة إيجابية.

اما المشرع الجزائري لم يشير الى جريمة انشاء موقع او حساب بشكل صريح انما شار الى التعامل في معطيات صالحة لارتكاب جريمة في نص المادة ٣٩٤ مكرر ٢ كتصميم البرامج الفيروسات المعلوماتية التي يمكن ان تستعمل في ارتكاب جرائم معلوماتية او ضد الأنظمة المعلوماتية او المعطيات المتمثلة في البيانات او المعلومات او انشاء مواقع لاستعمالها في جرائم نظم الاتصالات الالكترونية. [٢٨]

اما المشرع الفرنسي بموجب المادة (٣٢٣-٣-١) من قانون العقوبات المعدلة بالقانون رقم (٢٠١٣-١١٦٨) الخاص بالهجمات على نظم المعالجة الالية للبيانات التي نصت على "...او أي بيانات مصممة أو مكيفة خصيصا لارتكاب جريمة.." [٢٩]

نستنتج من نص هذه المادة ان المشرع الفرنسي لم ينص بصورة صريحة على جريمة انشاء موقع او حساب خاص بقصد ارتكاب جرائم نظم الاتصالات الالكترونية، وانما من مضمون التعبير تصميم برامج من اجل الوصول الى نظم المعالجة الالية او تصميم برامج لأهداف تخريبية مثل البرامج الفايروسية او انشاء مواقع لاستعمالها في جرائم نظم الاتصالات الالكترونية. [٣٠]

من خلال ما نص عليه المشرع في الدول محل المقارنة يتبين ان الافعال اتحدت في وصف السابق وجميعها صور إيجابية غير سلبية الا انها تختلف من حيث كونها تعد جرائم وقتية او جرائم مستمرة، حيث يعد فعل الانشاء او التصميم جريمة وقتية تقع كاملة بمجرد الانشاء او تصميم الموقع او الحساب دون الحاجة الى الاستمرار فيه، اما فعل ادارة الموقع او الحساب وفعل الاستخدام الحساب او الموقع يشتركون في كونهم جرائم مستمرة [٣١]، اذ تظل الجريمة قائمة في كل لحظة فيها الجاني يدير الحساب او الموقع او يستخدم حساب خاص او موقع خاص بقصد ارتكاب أفعال جرمها القانون. [٣٢]

ويجدر الإشارة الى ان هذه الجريمة التي تناولناها من الجرائم الشكلية أي انها تقع وتكتمل بمجرد وقوع الفعل المكون لها على نظم المعلوماتية، دون ان يتطلب المشرع في النص القانوني وحسب التجريم اية نتيجة إجرامية تترتب على الفعل المكون لها.

من خلال استقراء النصوص التشريعية لدول محل المقارنة يتبين ان محل الجريمة وفق ما نص عليه المشرع المصري والمشرع الاماراتي هو انشاء او إدارة او استخدام موقع او حساب خاص فقط. [٣٣]

اما محل الجريمة الذي خصه المشرع الجزائري والمشرع الفرنسي ففي صورتها الأولى وهي جرائم التعامل في معلومات صالحة لارتكاب جريمة، فهو يكمن حسب المادة (٣٩٤) مكرر ٢ من قانون العقوبات الجزائري في معلومات او البيانات المخزنة او معالجة الالية هي المعلومات المرسلة او تجهيزات او أدوات او البرامج والمعطيات خاصة بالمعالجة الآلية اما بخصوص المشرع الفرنسي حسب المادة (٣٢٣-٣-١) قانون العقوبات الفرنسي على ان تكون هذه الوسائل مصممة او معدة ومن ضمنها الموقع او الحساب المصمم خصيصا لارتكاب واحدة او أكثر من جرائم الاعتداء على نظم المعالجة الالية. (٣٤)

وعليه فان مجال تطبيق التجريم وفق المادة (٣٢٣-٣-١) مزدوج فمن جهة فان الأفعال الممثلة للسلوك الاجرامي المعاقب عليها متعلقة باستيراد او حيازة او توفير التجهيزات، الأدوات، المعدات... واي بيانات مصممة أي ان يكون انشاء هذه البيانات تم تصميمها كأنشاء موقع او حساب من اجل استخدامها، لارتكاب جريمة من جرائم الاعتداء على نظم المعالجة الالية.

اما اتفاقية بودابست لسنة ٢٠٠١ لقد اشارت الى مصطلحات التي تمثل السلوك الاجرامي للجريمة هو ما استخدمه المشرع الفرنسي في نص المادة (٣٢٣-٣-١) المعدلة بموجب القانون رقم (٢٠١٣- ١١٦٨) المؤرخ ١٨ ديسمبر ٢٠٢٣، ويتضح ذلك بشكل واضح من خلال الفقرة (٢) من نص المادة (٦) من الاتفاقية بودابست حيث نصت " أية أدوات أو برامج مصممة أو مكيفة لغايات ارتكاب الجرائم المبينة في المادة السادسة إلى المادة الثامنة". (٣٥)

**٢- الموقف التشريعي من التجريم:**

ان موقف المشرع في دول محل المقارنة اتجه الى عدة صور بالتجريم ، فالمشرع المصري جرم فعل انشاء او إدارة او استخدام موقع او حساب خاصا على شبكة معلوماتية وذلك من خلال المادة (٢٧) من قانون مكافحة جرائم تقنية المعلومات حيث نصت المادة على" في غير الأحوال المنصوص عليها في القانون يعاقب بالحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن

مائة ألف جنيه، ولا تزيد عن ثلاثمائة ألف جنيه، او بإحدى هاتين العقوبتين، كل من أنشأ او أدار او استخدم موقاً او حساباً خاصاً على شبكة معلوماتية يهدف الى ارتكاب او تسهيل ارتكاب جريمة معاقب عليها قانوناً"(٣٦).

ان غرض المشرع المصري في نص المادة (٢٧) هي مواجهة الخطورة الاجرامية المتمثلة في انشاء او إدارة او استخدام الموقع او الحساب الخاص بقصد ارتكاب الجرائم او تسهيل ارتكابها كنوع من أنواع الحماية الجنائية الاحترازية لمنع استخدامها في ارتكاب الجرائم بصفة عامة ، ان المشرع جعل ارتكاب الجريمة بشكل عام من خلال لفظة معاقب عليها قانونا، حيث ان ما نص عليه المشرع في المادة (١٨) من نفس القانون، انشاء واستخدام للموقع والحسابات الخاصة باسم الغير للأضرار به من خلال اتلاف او تعطيل او اختراق، اذا ان المادة (٢٧) اعم من المادة (١٨) حيث تمتد الجريمة في المادة (٢٧) الى كافة الجرائم وليس الاستخدام باسم الضحية او الغير الذي تم أنشاء الحساب باسمه بهدف إضراره ، كما ان المشرع المصري بقوله في غير الأحوال التي نص عليها هذا القانون جعل ضمنا ان انشاء حساب او موقع بغرض ارتكاب جرائم غير منصوص عليها في قانون رقم ١٧٥ لسنة ٢٠١٨ ، وذلك تجنبا من حالات التعدد المعنوي للجرائم حيث جعله نص احتياطي للجرائم تقنية المعلومات ، فاذا اخفق تحقق وانطباق أي من الجرائم وكان الجاني استعان بالوسائل الواردة في المادة (٢٧) فتكون هي محلا للتطبيق والعكس صحيح . (٣٧)

اما المشرع الفرنسي لقد جرم مجموعة أفعال تصب جميعها في التعامل بمعلومات التقنية التي تكون صالحة لارتكاب احدى جرائم التي تمس سرية المعلومات او سلامتها او اتاحتها، بموجب المادة (٣٢٣-٣-١) من قانون العقوبات المعدلة بموجب القانون رقم (٢٠١٣-١١٦٨) المؤرخ ١٨ ديسمبر٢٠١٣ الخاص بالهجمات على انظمة المعالجة الالية للبيانات التي نصت على "...او أي بيانات مصممة أو مكيفة خصيصا لارتكاب جريمة أو أكثر من الجرائم المنصوص عليها في المواد (٣٢٣-١) الى (٣٢٣-٣)، دون سبب مشروع، على الجريمة نفسها أو على الجريمة الأكثر عقوبة". (٣٨)

نستنتج من نص المادة أعلاه ان المشرع الفرنسي لم ينص بشكل صريح على تجريم انشاء حساب خاص او موقع خاص بغرض ارتكاب جريمة من جرائم تقنية المعلومات، وانما اعتبرها من ضمن البيانات المصممة او المكيفة خصيصا لارتكاب الجريمة او أكثر من الجرائم المنصوص عليها في القانون.

بخصوص المشرع الأمارتي جرم انشاء موقع او حساب خاص بموجب المادة (١٧) حيث نصت على " ... كل من أدار أو أنشأ أو استخدم موقعاً أو حساباً على شبكة معلوماتية يهدف إلى ارتكاب أو تسهيل ارتكاب جريمة معاقب عليها قانوناً". (٣٩)

اما المشرع الجزائري لقد جرم التصميم في معطيات مخزنة او معالجة او مرسلة عن طريق منظومة معلوماتية يمكن ان ترتكب بها جرائم من خلال المادة ٣٩٤ مكرر ٢ في القسم السابع مكرر (١) الخاص في المساس بأنظمة المعالجة الالية للمعطيات من قانون رقم (٦٦-١٥٦) المعدل حيث نصت المادة على " يعاقب بالحبس من شهرين (٢) الى ثلاث (٣) سنوات وبغرامة من (١٠٠٠,٠٠٠) مليون دينار جزائري الى (٥٠٠٠,٠٠٠) خمس ملايين دينار جزائري، كل من يقوم عمدا وعن طريق الغش بما يلي : ١- تصميم او بحث او تجميع او توفير او نشر او الاتجار في معطيات مخزنة او معالجة او مراسلة عن طريق منظومة معلوماتية يمكن ان ترتكب بها الجرائم المنصوص عليها في هذا القسم . ٢- حيازة او افشاء او نشر استعمال لاي غرض كان المعطيات المتحصل عليها من احدى الجرائم المنصوص عليها في هذا القسم." (٤٠)

ان المشرع الجزائري لم يحدد بشكل واضح تجريم انشاء موقع او حساب الكتروني خاص لغرض ارتكاب جرائم نظم الاتصالات او تقنية المعلومات حيث جرم بشكل واسع كل من قام بتصميم او بحث او تجميع او توفير او نشر او الاتجار في معطيات مخزنة او معالجة او مرسلة عن طريق منظومة معلوماتية، حيث ان المشرع استعمل مصطلح تصميم ويتمثل في اعداد وتكوين معلومات ضمن اطار معين صالحة لارتكاب الجريمة، وهذا عادةً يقوم به اشخاص لهم خبر ومتخصصون في المجال تقنية المعلومات، كمصممي البرامج حيث يتم تصميم برنامج معلوماتي من اجل ان يستخدم للوصول الى

نظم المعالجة الالية او تصميم برنامج من اجل ان يستخدم لتحقيق اهداف تخريبية كالبرامج الفايروسية، وكما يتضمن انشاء مواقع خاصة احترافية او بسيطة يمكن ان يتم استخدامها في الجرائم الالكترونية . (٤١)

وتطبيقا لذلك "قضت محكمة عنابة قسم الجنح بتوافر الجريمة في حق المتهم الذي قام بتصميم وانشاء مواقع وهمية شبيه بالمواقع الرسمية لبعض البنوك، وعند محاولة الزبائن اجراء عمليات الاتصال بحساباتهم المصرفية من اجل اجراء عمليات مصرفية بحساباتهم البنكية وجدوا أنفسهم في المواقع غير المقصودة والتي انشئها اشخاص مجرمين غير الجهة الحقيقية الرسمية للبنك، وبدون علم، وقد قام بتحويل مبلغ قيمته (١٠٠٠٠٠٠) دولار امريكي منذ سنة ٢٠٠٥، وكان كان اغلب ضحاياهم زبائن البنك الكندي". (٤٢)

اما ما ذهبت اليه الاتفاقية بودابست في المادة (٦) بخصوص إساءة استخدام الأجهزة "تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها لتجريم الافعال التالية في قانونها الوطني، إذا ما ارتكبت عمدا وبغير حق عملية انتاج او بيع او شراء ... لاي برنامج حاسوبي مصمم او معد خصيصا لغرض ارتكاب أي من الجرائم المقرر في المواد من (٢) الى (٥) من هذه الاتفاقية ... ويشير مصطلح توفير الأجهزة الى انشاء او تجميع وصلات تشعبية من اجل تيسير النفاذ الى هذه الأجهزة ويشير (ادراج برنامج حاسوبي) الى البرامج المصممة او المكيفة للحصول على إمكانية النفاذ الى أنظمة الكمبيوتر". (٤٣)

ومن خلال نص الاتفاقية بودابست ان هذه الجريمة تتمثل بعدة سلوكيات مثل تصميم البرامج الخبيثة كبرامج الفايروسات والبحث عن كيفية تصميمها او القيام بجمع المعطيات مثل كلمة السر الخاصة بالولوج الى جهاز الكمبيوتر واتاحتها الى الغير سواء كان بمقابل او بدون مقابل من اجل ارتكاب جريمة من جرائم نظم الاتصالات الالكترونية.

اما الاتفاقية العربية اشارت في المادة التاسعة في الفقرة (١) التي نصت على " إنتاج ... توزيع أو توفير :أ – أية أدوات أو برامج مصممة أو مكيفة لغيات ارتكاب الجرائم المبينة في المادة السادسة إلى المادة الثامنة. ب– كلمة سر نظام معلومات أو شيفرة دخول او معلومات مشابهة يتم بواسطتها دخول نظام معلومات ما بقصد استخدامها ألية من الجرائم المبينة في المادة السادسة إلى المادة الثامنة". (٤٤)

وخلاصة القول ان التشريعات في الدول المقارنة لم يكن لها موقف محدد في جريمة الانشاء حيث اخذ المشرع المصري والمشرع الاماراتي بتجريم انشاء موقع خاص او حساب خاص لارتكاب جرائم تقنية المعلومات والاتصالات الالكترونية بينما اتجه المشرع الفرنسي والمشرع الجزائري الى تجريم صورتين الأولى تجريم التعامل في معلومات صالحة لارتكاب جريمة والثانية التعامل في معلومات متحصلة من جريمة والمتمثلة بالأفعال (تصميم او بحث او تجميع او توفير او نشر او الاتجار) في معطيات مخزنة او معالجة او مرسلة عن طريق منظومة معلوماتية يمكن ان ترتكب بها جرائم، وكما ان المشرع الفرنسي لقد جرم مجموعة أفعال تصب جميعها في التعامل بمعلومات التقنية التي تكون صالحة لارتكاب احدى جرائم التي تمس سرية المعلومات او سلامتها او اتاحتها.

نستنتج من خلال استقراء التشريعات في الدول محل المقارنة ، ان المشرع حدد صور عديدة للجريمة، حيث ان المشرع المصري عدد صور الجريمة لتشمل ثلاث صور، وهي انشاء موقع او حساب خاص ، وإدارة موقع او حساب خاص ، واستخدام موقع او حساب خاص ، بهدف ارتكاب جرائم تقنية المعلومات ، وكذلك المشرع الاماراتي حدد صور عديدة للجريمة ، وهي انشاء موقع، وإدارة موقعا إلكترونيا، و الاشراف عليه، اما المشرع الجزائري كذلك فعل عدد صور عديدة في ارتكاب الجريمة حيث اخذ بشكل أوسع، حيث نص كل من يقوم عمدا وعن طريق الغش بما يلي، تصميم او بحث او تجميع او توفير او نشر او الاتجار في معطيات مخزنة او معالجة او مرسلة عن طريق منظومة معلوماتية يمكن ان ترتكب بها جرائم، وكذلك المشرع الفرنسي جرم عدة صور للجرمية من

خلال قوله يعاقب على استيراد أو حيازة أو عرض أو نقل أو إتاحة معدات أو أداة أو برنامج حاسوبي أو أي بيانات مصممة أو مكيفة خصيصا لارتكاب جريمة.

نرى من الاجدر على المشرع في الدول المقارنة، ان يحدد الأفعال المجرمة بشكل دقيق وعدم الاسهاب بالألفاظ التي في اغلب التشريعات تؤدي الى مدلول واحد، وان ويفرز كل سلوك اجرامي عن الاخر في فقرة او مادة مستقلة ويبين من خلال الوصف الدقيق للسلوك الاجرامي الركن المادي والركن المعنوي، ويضع العقوبة المناسبة كل واحد منها، والاخذ بما اشارت اليه الاتفاقية العربية واتفاقية بودابست بشكل موحد من اجل ان يؤدي ذلك الى تعزيز التعاون الدولي لمكافحة جرائم الاتصالات الالكترونية والتي من سماتها هي عابرة للحدود.

اما المشرع العراقي لم يتطرق الى جريمة انشاء موقع او حساب لارتكاب جرائم نظم الاتصالات الالكترونية في قانون العقوبات رقم ١١١ لسنة ١٩٦٩ المعدل وكذلك لم يتطرق لها مشروع قانون مكافحة الجرائم الالكترونية لسنة ٢٠١٩ وبذلك يكون هناك قصور تشريعي يجب ان ينتبه اليه المشرع العراقي من اجل سد هذا القصور من خلال تعديل قانون رقم ١١١ لسنة ١٩٦٨ او اصدار تشريع جديد يتضمن حماية جنائية احترازية لمنع جرائم نظم الاتصالات الالكترونية.

نرى ان القضاء العراقي في حالة عرض وقائع جريمة التي تتمثل بفعل اشاء موقع او حساب خاص يذهب القضاء بتطويع قانون العقوبات رقم ١١١ للوقائع من اجل ان تتلاءم الوقائع مع نص القانون الذي يخلو من تجريم فعل انشاء موقع او حساب خاص لارتكاب جريمة كما في بخصوص قضية انشاء المتهم موقع وهمي باعتباره من جرائم التزوير حيث قضت محكمة استئناف محكمة المثنى بصفتها التمييزية في قرارها رقم ٥٧/ت ج / ٢٠١٩ في ٢٠١٩/٣/٣١ بحق المدان لأحكام المادة ٣٦٣ من قانون العقوبات لسنة ١٩٦٩ المعدل وحكمت عليه بغرامة خمسمائة الف دينار حيث نص القرار التمييزي "لدى التدقيق و المداولة وجد ان الطعن التمييزي مقدم ضمن المدة القانونية قرر

قبوله شكلا و لدى عطف النظر على القرار المميز وجد انه غير صحيح و مخالف للقانون لان محكمة الجنح و من قبلها محكمة التحقيق قد اخطأتا في التكييف القانوني السليم لفعل المتهم يشكل صورة من صور التزوير وبما ان المادة ٢٨٦ من قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩ المعدل وما يعزز هذا الاتجاه ويسنده ما ورد في المادة (١/عاشرا ) من قانون التوقيع الالكتروني و المعاملات الالكترونية رقم (٧٨) لسنة ٢٠١٢ وقد عرفت المستندات الالكترونية بانها المحررات و الوثائق التي تنشا او تبرمج او تخزن او ترسل او تستقبل بوسائل الكترونية بما في ذلك تبادل البيانات وعلى هذا الأساس لابد من مواكبة التطورات الحاصلة في مجال تكنولوجيا المعلومات والاتصالات وأنشطة الانترنت بما ينسجم والتطورات القانونية في الحوادث الالكترونية وتطويع النص القانوني التقليدي بما يتلائم مع تلك الحوادث وحيث ان المتهم لم يقم بتحريف الصفحة الشخصية الحقيقية للمشتكي وانما اصطنع صفحة جديدة له غير حقيقية ونسبها للمشتكي بقصد الاضرار به وبذلك يكون فعله ينطبق واحكام المادة (٢٩٢) من قانون العقوبات رقم ١١١ لسنة ١٩٦٩ المعدل وبما ان المتهم أيضا قد استخدم ذلك التطبيق فقد ارتكب فعلا اخر وهو الاستعمال وفق احكام المادة (٢٩٨) من قانون العقوبات وبدلالة المادة (٢٩٢ ) من ذات القانون باعتبارها جرائم ناتجة عن أفعال مرتبطة ببعضها ارتباطا يجمع بينها غرض واحد وفق احكام المادة (١٣٢) من قانون أصول المحاكمات الجزائية رقم ٢٣ لسنة ١٩٧١ المعدل عليه ولكل ما تقدم تقرر نقض كافة القرارات الصادرة في الدعوى وإعادة الدعوى الى محكمة التحقيق..".[٤٥]

وعلى هذا الاساس نرى ان القضاء العراقي يعمل على تطويع النص القانوني التقليدي من اجل ان يتلائم مع السلوك الاجرامي الذي لم ينص عليه القانون حيث ان المتهم لم يقوم بتحريف الصفحة الشخصية للمشتكي وانما انشاء حساب خاص غير حقيقي ونسبه للمشتكي بقصد الاضرار به، لذا نرى على المشرع العراقي ان يبادر الى تعديل القانون او اصدار قانون جديد يواكب التطور التكنولوجي لغيطي القصور الحاصل في قانون العقوبات التقليدي التي لا يتلائم مع السلوك الاجرامي في الفضاء الالكتروني وخصوصا الاتصالات الالكترونية.

## الخاتمة

بعد الانتهاء من البحث توصلنا الى العديد من الاستنتاجات والمقترحات التي توصلنا اليها وهي كما يأتي:

### أولا: الاستنتاجات

١- لم ينص المشرع العراقي على حماية نظم الاتصالات الالكترونية حماية جنائية احترازية في قانون العقوبات رقم ١١١ لسنة ١٩٦٩ المعدل، حيث نص المشرع في مصر وفرنسا والجزائر والامارات عليها، من اجل الوقاية من جرائم نظم الاتصالات من الاعتداء قبل وقوع الجريمة.

٢- لم ينص المشرع العراقي على تجريم حيازة او تداول الأجهزة والمعدات لارتكاب جرائم نظم الاتصالات الالكترونية في قانون العقوبات العراقي، كما ان المشرع في الدول المقارنة لم يتفق على صورة موحدة للجريمة ولم يشترط الضرر الفعلي على المجني عليه ولكن يتطلب لوقوع جريمة التداول وحيازة الأجهزة والمعدات والآلات الخاصة بارتكاب جرائم نظم الاتصالات الالكترونية، كما ان الاماراتي والمشرع الجزائري ذهب الى تجريم الأشياء المعنوية كالبرامج المعلوماتية او أي وسيلة تقنية معلومات التي يمكن ان يتم بواسطتها ارتكاب الجريمة، ولم يجرم حيازة او تداول او استخدام الأشياء المادية مثل الأجهزة والمعدات التي يمكن ان تستخدم في ارتكاب الجريمة كما فعل المشرع الفرنسي والمشرع المصري.

٣- لم ينص المشرع العراقي على عقوبة انشاء او إدارة او استخدام موقع او حساب خاص او بريد الالكتروني لارتكاب الجرائم الخاصة بنظم الاتصالات الالكترونية في قانون العقوبات رقم ١١١ لسنة ١٩٦٩ ، كما ان الحال في الدول محل المقارنة لم يكن هناك تناسب بين صور التجريم وبين العقوبات المترتبة عليها ، حيث ساوى المشرع المصري بين انشاء موقع وبين من يقوم بإدارة الموقع وكذلك ساوى بينهم وبين من يستخدم الموقع او حساب لغرض ارتكاب الجريمة ،

كان من الاجدر عدم خلط بين الانشاء والإدارة والاستخدام بخصوص المشرع المصري، والتصميم والحيازة او العرض او النقل او الاتاحة بخصوص المشرع الفرنسي ، كما ان المشرع الفرنسي ساوى التداول في معدات والأدوات والبرامج.

**ثانيا: المقترحات:**

١- لمعالجة إساءة استخدام الأجهزة والمعدات الخاصة في نظم الاتصالات كحماية جنائية احترازية لنظم الاتصالات الالكترونية نقترح إضافة النص التالي:

يعاقب بالحبس مدة لا تقل عن ثلاثة سنوات ولا تزيد على خمس سنوات وغرامة لا تقل عن (٣٠٠٠,٠٠٠) ثلاثة ملايين ولا تزيد عن (١٠,٠٠٠,٠٠٠) او احدى هاتين العقوبتين كل من حاز او أحرز او تداول او صمم او أنتج او استورد او أتاح أي برنامج معلوماتي او وسيلة تقنية معلومات او شفرات او رموز او أي معدات تقنية أخرى بقصد ارتكاب او تسهيل ارتكاب جريمة من جرائم المنصوص عليها في هذا القانون.

٢- ونقترح ولمعالجة انشاء موقع حساب خاص او بريد الكتروني النص التالي:

أ- يعاقب بالحبس مدة لا تقل عن سنتين ولا تزيد على خمس سنوات وغرامة لا تقل عن (٥٠٠٠,٠٠٠) خمسة ملايين دينار عراقي، كل من انشاء لغيره موقعا او حسابا او بريد الكتروني على شبكة معلوماتية يهدف الى ارتكاب او تسهيل ارتكاب جريمة يعاقب عليها قانوناً.

ب-وتكون العقوبة السجن مدة لا تقل عن سنوات وغرامة لا تقل عن (١٠,٠٠٠,٠٠٠) عشرة ملايين دينار عراقي، كل من أنشأ واستخدم او ادار الموقع او الحساب بهدف ارتكاب جريمة يعاقب عليها قانوناً.

(١) ينظر: المادة (٢٢) من قانون رقم ١٧٥ لسنة ٢٠١٨ المصري بشأن مكافحة جرائم تقنية المعلومات.

(٢) ينظر: الفقرة (١) من المادة (٢٢٦-٣) المعدلة بموجب قانون رقم ٩٣٦-٢٠٢٠ المؤرخ في ٣٠ يوليو ٢٠٢٠.

(٣) ينظر: المادة (١٤) من قانون رقم (٥) لسنة ٢٠١٢ الاماراتي بشأن مكافحة جرائم تقنية المعلومات.

(٤) ينظر: المادة (٣٩٤) مكرر (٢) من القسم السابع مكرر الخاص بالمساس بأنظمة المعالجة الالية للمعطيات من قانون (٦٦-١٥٦) المعدل والمتمم لسنة ٢٠١٢.

(٥) ينظر: محمد جمال رجب الحاوي، الحماية الجنائية للاتصالات الالكترونية في العصر الرقمي دراسة مقارنة، دار الجامعة الجديدة، الإسكندرية ،٢٠٢٣، ص٣٦٤.

(٦) ينظر: المستشار احمد محمود موافي، احكام قانون مكافحة جرائم تقنية المعلومات، الطبعة الثانية، دار الاهرام للنشر والتوزيع والاصدارات القانونية، المنصورة، ٢٠٢٢، ص٤٧٢.

(٧) ينظر: المستشار وجدي شفيق فرج، د. لوفيرا النجار، شرح قانون تقنية المعلومات والتوقيع الإلكتروني وتنظيم الاتصالات في ضوء اللوائح التنفيذية والقرارات الوزارية والاتفاقية العربية لمكافحة جرائم تقنية معلومات ومبادئ القسم العام لقانون العقوبات وقضاء محكمة النقض واحداث احكام المحكمة الاقتصادية ومذكرات الدفاع والدفوع في جرائم تقنية المعلومات، دار الاهرام للنشر وتوزيع الإصدارات القانونية، القاهرة ،٢٠٢٢، ص٦٥٤.

(٨) ينظر: المستشار وجدي شفيق فرج، لوفيرا النجار، المصدر السابق، ص٦٥٤.

(٩) ينظر: محمد جمال رجب الحاوي، المصدر السابق، ص٣٦٤.

(١٠) ينظر: سمير عوض محمود، اثبات جرائم الانترنت دراسة مقارنة، الطبعة الأولى، دار النهضة العربية للنشر والتوزيع، القاهرة، ٢٠٢٠، ص١٩٨.

(١١) ينظر: د. محمود نجيب حسني، مصدر سابق، ص٣٦٤ وما بعدها.

(١٢) ينظر: رشيدة بوكر، الحماية الجزائية للتعاملات الالكترونية، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، ٢٠٢٠، ص١١٦.

(١٣) ينظر: المادة (٢٢) من قانون المصري رقم ١٧٥ لسنة ٢٠١٨ بخصوص مكافحة جرائم تقنية المعلومات.

(١٤) ينظر: محمود رجب فتح الله، شرح قانون مكافحة جرائم تقنية المعلومات في ضوء القانون المصري ١٧٥ لسنة ٢٠١٨ دراسة مقارنة، دار الجامعة الجديد للنشر، الإسكندرية، ٢٠١٩، ص٧٦٤.

(١٥) ينظر: الفقرة (١) من المادة (٢٢٦ -٣) من قانون العقوبات الفرنسي المعدلة بموجب قانون رقم (٩٣٦-٢٠٢٠) لسنة ٢٠٢٠ المؤرخ ٣٠جويليه ٢٠٢٠.

(١٦) ينظر: الفقرة (٢) من المادة (٢٢٦ -٣) من قانون العقوبات الفرنسي المعدلة بموجب قانون عدد ٩٣٦ لسنة ٢٠٢٠ المؤرخ ٣٠ يوليو ٢٠٢٠.

(١٧) ينظر: المادة (١٦) من قانون رقم (٣٤) لسنة ٢٠٢١ بشأن مكافحة الشائعات والجرائم الالكترونية.

(١٨) ينظر: عبد الرزاق الموافي عبد اللطيف، قراءة قانون مكافحة جرائم تقنية المعلومات الاماراتي الجديد، مجلة معهد دبي القضائية، العدد ٢، السنة الأولى، مارس ٢٠١٣، ص١٥٦.

(١٩) ينظر: المادة ٣٩٤ مكرر ٢ من القسم السابع المكرر الخاص بالمساس بأنظمة المعالجة الالية للمعطيات من قانون رقم (٦٦-١٥٦) المعدل والمتمم لسنة ٢٠١٢

(٢٠) ينظر: د. احمد برادي، آليات مكافحة الجريمة الالكترونية في ضوء قانون العقوبات الجزائري، مجلة وميض الفكر، للبحوث، أيلول، ٢٠٢٠، ص٤٥٨.

(٢١) ينظر: الفقرة (١) المادة (٦) من الاتفاقية بودابست المكافحة جرائم الالكترونية سنة ٢٠٠١.

(٢٢) ينظر: الفقرة (٢) من المادة (٦) من اتفاقية بودابست بخصوص مكافحة الجريمة الالكترونية لسنة ٢٠٠١.

(٢٣) ينظر: الفقرة (٥) والفقرة (٦) من المادة (٦) من اتفاقية بودابست بخصوص مكافحة الجريمة الالكترونية لسنة ٢٠٠١.

(٢٤) ينظر: الفقرة (٣) من المادة (٦) من اتفاقية بودابست

(٢٥) ينظر: المادة (٩) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المبرمة في القاهرة سنة ٢٠١٠.

(٢٦) ينظر: د. محمد جمال رجب الحاوي، مصدر سابق، ص٣٥٠.

(٢٧) ينظر: عمر محمود الحوتي، الوجيز في الحماية الجنائية من جرائم تقنية المعلومات وفق احكام القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات، دار النهضة العربية، ٢٠٢٠، ص١٨٥وما بعدها.

(٢٨) ينظر: نسيم دردور، جرائم المعلوماتية على ضوء القانون الجزائري والمقارن، رسالة ماجستير مقدمة الى جامعة منتوري (قسنطينة) كلية الحقوق، لسنة ٢٠١٢- ٢٠١٣، ص٣٦.

(٢٩) ينظر: المادة (٣٢٣-٣-١) من قانون العقوبات الفرنسي المعدلة بقانون رقم ٢٠١٣-١١٦٨ لسنة ٢٠١٣.

(٣٠) ينظر: د. رشيد بوكر، مصدر سابق، ص١٠٩.

[٣١] ينظر: د. عبد الفتاح الصيفي، جلال ثروت، القسم العام في قانون العقوبات، منشأة دار المعارف، ٢٠٠٥، ص٢٧٩.

[٣٢] ينظر: د. محمد جمال رجب الحاوي، مصدر سابق، ص٣٨٧.

[٣٣] ينظر: راجع نص المادة (٢٧) من قانون مكافحة جرائم تقنية المعلومات المصري والمواد (٢٣ و٢٤و٢٥و ٢٧ و٢٨) من قانون مكافحة جرائم تقنية المعلومات الاماراتي.

[٣٤] ينظر: المادة ٣٩٤ مكرر ٢ من القانون الجزائري والمادة المادة (٣٢٣-٣-١) قانون العقوبات الفرنسي.

[٣٥] ينظر: الفقرة (أ) من المادة (٩) من اتفاقية بودابست

[٣٦] ينظر: المادة (٢٧) من قانون المصري رقم ١٧٥ لسنة ٢٠١٨ لمكافحة جرائم تقنية المعلومات.

[٣٧] ينظر: د. محمد جمال رجب الحاوي، مصدر سابق، ص٣٨٢.

[٣٨] ينظر: المادة (٣٢٣-٣-١) من قانون العقوبات الفرنسي المعدلة بقانون رقم ٢٠١٣-١١٦٨ لسنة ٢٠١٣.

[٣٩] المادة (١٧) من قانون الاماراتي رقم (٣٤) لسنة (٢٠٢١) بشأن مكافحة الشائعات والجرائم الالكترونية..

[٤٠] ينظر: المادة (٣٩٤) مكرر ٢ القسم السابع مكرر ١ المساس بأنظمة المعالجة الالية للمعطيات من المرسوم بقانون رقم (٦٦-١٥٦) العقوبات الجزائري المعدل والمتمم سنة ٢٠١٢.

[٤١] ينظر: دردور نسيم، مصدر سابق، ص٣٦-٣٧.

[٤٢] ينظر: محكمة عنابة، قسم الجنح، رقم ٠٧٣٥٧/١٠ بتاريخ ٢٠١٠/٦/٢٨ قضية جنحة تصميم وإدخال عمدا وعن طريق الغش لمعطيات للمعالجة الالية والمتاجرة فيها أدت الى تعديل معطيات تلك المنظومة وجنحة التقليد وجنحة السرقة ضد (ف محمد)، للاطلاع راجع د. رشيدة بوكر، مصدر سابق، ص١٠٩.

[٤٣] ينظر: المادة (٦) من الاتفاقية بودابست لسنة ٢٠٠١ بشأن مكافحة الجريمة الالكترونية.

[٤٤] ينظر: الفقرة (١) من المادة (التاسعة) من الاتفاقية العربية لسنة ٢٠١٠ بشأن مكافحة الجرائم تقنية المعلومات.

[٤٥] ينظر: حكم محكمة استئناف المثنى بصفتها التمييزية رقم ٥٧/ ت ج/ ٢٠١٩ في ٣١ /٣ /٢٠١٩ بخصوص جريمة انشاء المتهم موقع الكتروني وهمي.