مجلة الحقوق والحريات
المجلد 12 ، العدد 1
السنة 2024 ، ص262-ص279

تحديات كشف الهوية الالكترونية للجناة: بين أساليب التمويه والحواجز القانونية

Challenges in Uncovering Electronic Identity of Criminals: Between Camouflage Methods and Legal Barriers

بن فرحات نورالدين [1] عمري عبد القادر [2]

[1] كلية الحقوق- جامعة يحي فارس- المدية (الجزائر)
benferhat.noureddine@univ-medea.dz

[2] كلية الحقوق- جامعة يحي فارس- المدية (الجزائر)
Avocat.amri@yahoo.fr

تاريخ الارسال:	تاريخ القبول:	تاريخ النشر:
2024/01/21	2024/03/25	2024/04/05

الملخص:

ان مكافحة الجرائم الإلكترونية، يحتاج الى تحديد الهوية الالكترونية للجناة، عن طريق نظام البصمات الالكتروني وتقنيات التشفير، لمعرفة مواقع الأجهزة المستخدمة عن طريق بروتوكول الإنترنت(TCP/IP).

الكلمات المفتاحية:

مكافحة الجرايم الاكترونية، الهوية الالكترونية للجناة، نظام البصمات الاكتروني، تحديد مواقع الأجهزة، بروتوكول الإنثرنت (TCP/IP)، تقنيات التشفير.

Abstract:

Fighting cybercrimes encounters challenges in pinpointing device locations amid TCP/IP complexities. Criminals exploit encryption, emphasizing scrutinizing codes for investigations.

key words:

Combating Electronic Crimes, Electronic Fingerprint System, Device Location Determination, Internet Protocol (TCP/IP),Electronic Identity of the Perpetrator ,Encryption Techniques.

المؤلف المرسل : بن فرحات نور الدين

مقدمة:

في ساحة التحقيقات الرقمية لمكافحة الجرائم الإلكترونية، ندخل متاهة معقدة حيث تتداخل التكنولوجيا والجريمة بشكل لا يُسهّل التمييز بين خطوط الحقيقة والخيال. يُجسّد المجرم الإلكتروني في عصرنا الحالي فنونًا متقدمة من التشفير والاختباء الرقمي، مما يضع التحقيقات القانونية في تحديات فريدة ومتزايدة.

تتجلى براعة المجرمين الإلكترونيين في استخدام التشفير والشفرات الرياضية المعقدة لتحويل البيانات إلى لغة غير مفهومة، وبالتالي يصبح التحليل والكشف عن الأدلة أمرًا غاية في الصعوبة. يتسارع هذا التقدم التكنولوجي مع تزايد التحقيقات في ميدان مكافحة الجرائم الإلكترونية، ما يعزز التحديات التي تواجه السلطات القانونية في الحفاظ على العدالة والكشف عن الجرائم الرقمية.

تفجر هذه الساحة الرقمية تحديات متنوعة، تبدأ من تحديد هوية الجاني وترجمة مختلف تقنيات التشفير، وتنتهي بتقديم الأدلة الرقمية التي تُضاء بها القضايا. لذا، تأتي هذه الدراسة لاستكشاف أعماق هذا الميدان المعقد وتسليط الضوء على الأساليب الفعّالة لمكافحة جرائم الأمان السيبراني. يهدف البحث أيضًا إلى توضيح الأساليب والأدوات المستخدمة في مواجهة التهديدات الرقمية، مع التركيز على تحسين القدرات التحقيقية وتطوير استراتيجيات مبتكرة للتصدي للتحديات الرقمية الناشئة.

وبينما نسعى لفهم عمق هذا المجال، نواجه إشكالية تحديد عنوان المجرم الإلكتروني أمام تلك التطورات التكنولوجية السريعة وضرورة مواكبتها. هنا يكمن التحدي الأكبر: **كيف يمكن تحسين عمليات تحديد عناوين المجرمين الإلكترونيين في ظل استخدامهم للتشفيروتقنيات الهويات المزيفة؟**

اتبعنا في إجابتنا على هذه الاشكالية منهج من المناهج المعتمدة في الدراسات القانونية، هو المنهج الوصفي، لوصف صعوبة وأدوات تحديد عنوان المجرم الاكتروني، وكذا شرح مدى فعالية هذه الأدوات لكشف هوية الجناة والقبض عليهم.

نقسم هذه الدراسة الى قسمين:

المبحث الأول: صعوبة تحديد عنوان المجرم الاكتروني

المبحث الثاني: فرض الجناة لتدابير أمنية

المبحث الأول: صعوبة تحديد عنوان المجرم الإلكتروني

في سياق التحقيقات لمكافحة الجرائم الإلكترونية، نشهد تحديات كبيرة في محاولة تحديد مواقع الأجهزة المستخدمة في الأنشطة الإجرامية. يستند نظام البصمات الإلكتروني على تتبع الحركة العكسية للمسارات عبر الإنترنت وتحديد العنوان الرقمي (IP) كوسيلة رئيسية لتحديد موقع الحاسوب. في هذا السياق، نتعامل أولاً مع تحديات عمل بروتوكول الإنترنت (TCP/IP)، حيث تتسارع التعقيدات في حالات الصيد الإلكتروني واستخدام الهويات المزيفة، مما يجعل من الصعب تحديد هوية الجاني. يتناول النص أيضًا المؤتمر الدولي حول جرائم الحواسيب، الذي يلقي الضوء على صعوبات الكشف عن هوية الجانيين في بيئة الإنترنت المعقدة، ويسلط الضوء على دور الأدلة والذكاء القضائي في التصدي لهذه التحديات. بالإضافة إلى ذلك، نقوم بتسليط الضوء على الموقف الفرنسي في استخدام بروتوكول الإنترنت لتحديد عنوان المجرم الإلكتروني، ونناقش الدور المحتمل للدول في الكشف عن هويات ناشري المحتوى عبر الإنترنت. لهذا سنتطرق من خلال هذا المبحث الى أدوات تحديد عنوان المجرم الاكتروني (المطلب الأول)، والى فعالية أدوات تحديد عنوان المجرم الاكتروني (المطلب الثاني).

المطلب الأول: أدوات تحديد عنوان المجرم الالكتروني

في ظل التحقيقات المتعلقة بمكافحة الجرائم الإلكترونية، يظهر تحديات كبيرة في تحديد موقع الأجهزة المستخدمة في الأنشطة الإجرامية. يُستخدم نظام البصمات الإلكتروني لتتبع الحركة العكسية للمسارات عبر الإنترنت وتحديد العنوان الرقمي (IP)، الذي يعد وسيلة رئيسية لتحديد موقع الحاسوب. يعتمد النظام على بروتوكولات مثل TCP/IP، لكن التحديات تنشأ عندما يتم استخدام الهويات بطرق غير قانونية أو عندما يتغير العنوان بكل اتصال. تلك التحديات تبرز في حالات قانونية، حيث قد لا يكون العنوان الرقمي دليلاً قاطعًا لتحديد هوية الجاني بشكل دقيق، لهذا وللاحاطة بأدوات تحديد عنوان المجرم الالكتروني نتطرق الى بروتوكول الإنترنت (TCP/IP) (الفرع الأول) والى نظام عمل بروتوكول الإنترنت (TCP/IP) (الفرع الثاني).

الفرع الأول: بروتوكول الإنترنت (TCP/IP)

في مواجهة التحقيقات لمكافحة الجرائم الإلكترونية، تظهر تحديات كبيرة، ومنها تعقيدات في تحديد مكان تواجد جهاز الحاسوب الذي يكون مصدرًا للنشاط الإجرامي. يتم التحقيق عادة باستخدام نظام فحص إلكتروني يُعرف بعلم البصمات المعاصر.[1]

هذا النظام يعتمد على تتبع الحركة العكسية لمسار الإنترنت أو التحقق من الحركة التراسلية للنشاط عبر الإنترنت بهدف تحديد عنوان رقمي للجهاز، والذي يُسمى بعنوان بروتوكول الإنترنت adresse internet protocole يتألف العنوان الـ IP من جزئين، الأول يشمل أرقام الشبكة والثاني يشمل أرقام مقدم الخدمة، هذا النظام يُمكن من التعرف على الجهاز المتصل بشبكة الإنترنت عن طريق عناوين عددية فريدة. بالتالي، يعتبر عنوان الـ IP وسيلة رئيسية لتحديد موقع الحاسوب المستخدم في ارتكاب الجريمة الإلكترونية.[2]

تستند السلطات التحقيق على هذا النظام للوصول إلى موقع الجهاز، وهو أمر أساسي للكشف عن الجاني. إذ يسهم علم البصمات المعاصر في فهم الحركات والتفاعلات عبر الإنترنت، وبناءً على ذلك، يُمكن للسلطات القانونية معاقبة المتسببين في الأنشطة الجرمية الإلكترونية بموجب القوانين الصادرة في هذا السياق.

الفرع الثاني: نظام عمل بروتوكول الإنترنت (TCP/IP)

بروتوكول الإنترنت (IP) يتفاعل بشكل متزامن مع بروتوكول آخر يُعرف ببروتوكول التحكم بالنقل(TCP) ، وهما جزء لا يتجزأ من عائلة بروتوكولات .TCP/IP هذه العائلة تهدف إلى تسهيل نقل البيانات بين أنظمة الحواسيب، وقد اعتبر نظام UNIX[3] المعيار الرئيسي للبيانات الرقمية عبر شبكة الإنترنت،

[1] بفضل هذا النظام تم الكشف عن العديد من المجرمين مثل مبتكر فيروس ميليسا و مبتكر موقع خدمات بولمبروج الأخبار المال الاحتيالي الذي يرفع الأسهم عن طريق الخداع.

[2] عبد الحميد عبد المطلب، استخدام برتوكول (TCP/IP) في بحث و تحقيق الجرائم على الكمبيوتر، 15-1-2019، 1-12-2023، منشور على الموقع الالكتروني www.arablaw.info.com.

[3] (UNIX) هو نظام تشغيل متعدد المهام صمم لاستخدامه في الحاسب المنزلي أو المكتبي باعتباره مكتوب باللغة(C) ، وهي لغة برمجة عالية المستوى صممت خصيصا لتعمل وفق نظام (UNIX) ، وتستخدم في كتابة كافة التطبيقات بعد أن وضع مقاييسها من طرف المعهد القومي الأمريكي للمقاييس، لذلك بعد نظام (UNIX) الأكثر قابلية للنقل المعلوماتي من الأنظمة الأخرى.

بروتوكول الإنترنت (IP) وبروتوكول التحكم بالنقل (TCP) يعتمدان على تقنية التبديل المعلوماتي باستخدام الحزم المعلوماتية (Pocket) بين الوصلات السلكية واللاسلكية المتخصصة. تُشكل الحزمة المعلوماتية ملفًا ثابت الحجم، يحمل رقمًا خاصًا ومعلومات تعريفية عن الحاسوب المرسل والحاسوب المستقبل. في كل وصلة، يُقرأ مصدر الحزمة ويُعيد إرسالها عبر الوصلات نحو الهدف أو المرسل النهائي.[1]

هذا التبديل المعلوماتي يسهم في تسهيل نقل البيانات بفعالية بين الأنظمة. الحزمة المعلوماتية تحمل معها معلوماتٍ تحديديةً، مما يُيسّر قراءة ومعالجة الحزم عبر الوصلات المختلفة. بروتوكول الإنترنت (IP) وبروتوكول التحكم بالنقل (TCP) يشكلان تركيبة أساسية للتواصل الفعّال بين الحواسيب والأنظمة في بيئة الشبكات، مع تحقيق استقرار الاتصالات وتوجيه الحزم بشكل آمن وفعّال نحو وجهتها المقصودة

في حال استخدام نظام (TCP/IP) للكشف عن مصدر جهاز يقوم بارتكاب جريمة إلكترونية وتحديد موقعه، يُعَدّ هذا النهج وسيلة مؤثرة. ومع ذلك يجب أن ندرك أن النتائج التي يمكن الوصول إليها لا تكون دائمًا دقيقة وجادة. يتم تحديد مصدر الجريمة عادة بواسطة عنوان الإنترنت(IP) ، ولكن هذا لا يكون كافيًا لتحديد هوية صاحب الجهاز بدقة. الحاسوب قد يكون مسروقًا أو يستخدم في أماكن عامة، وعنوان الإنترنت قد يكون مستخدمًا بشكل غير قانوني.[2]

في قضية فوريسيوا، التي تعتبر واحدة من القضايا الشهيرة المتعلقة بالجرائم الإلكترونية، كان النقاش حول نشر رسالة إلكترونية عنصرية على الموقع الإلكتروني (Aaargh)الذي يستضيف في الولايات المتحدة. تبعًا للمحكمة الفرنسية، عندما تمت مقاضاة الشخص الذي كتب الرسالة، كانت المحكمة غير قادرة على تقديم دليل قاطع يثبت أن المتهم هو الشخص الفعلي الذي نشر الرسالة الجريمة.[3]

---

[1] عبد الحميد عبد المطلب، مرجع سابق، ص 01.

[2] راسل تاينر، أهمية التعاون الدولي في منع جرائم الانترنت، بحث مقدم إلى الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، الجارية بالمملكة المغربية، في الفترة 19 و 20 جوان 2007، ص ص 113-114.

[3] T.G.I. novembre, 1998, disponible a l'adresse suivant;
http://www.legalis.jnet.decision/illicite -divers/correct-Paris-1998-htm.

عليها أن تأخذ في اعتبارها أن وجود اسم المتهم في نهاية الرسالة لا يُعتبر بالضرورة دليلاً قاطعًا على كونه مصدر الرسالة. وقد قررت المحكمة أن يمكن لأي شخص كتابة هذا الاسم انطلاقًا من نية التمويه، وبالتالي، لا يُعتبر دليلاً كافيًا للإدانة .

هذا يسلط الضوء على التحديات التي تواجه عمليات تحديد هوية الجاني في العالم الرقمي، حيث قد يتم استخدام الهويات بطرق غير قانونية أو قد يتورط الأشخاص في استخدام حواسيبهم بطرق لا تعكس تصرفاتهم الفعلية.

يُظهر بروتوكول الإنترنت (TCP/IP)، الذي يستند إلى عناوينIP ، أنه ليس موحدًا على مستوى عالمي ويمكن أن يتغير مع كل اتصال. يُبرز أن كل عنوان IP يتعارض مع عدة هويات، مما يؤكد على التحديات المتعلقة بتحديد هوية الفاعل في البيئة الرقمية.[1]

المطلب الثاني: تحديات العمل ببروتوكول الإنترنت (TCP/IP)

في مجال مكافحة الجرائم الإلكترونية، تظهر تحديات كبيرة في تحديد هوية الجاني في بيئة الإنترنت باستخدام بروتوكول الإنترنت (TCP/IP). تضهر صعوبات تحديد هوية الفاعل بسبب تغيرات متكررة في عناوين IP، مع التركيز على التحديات المتعلقة باستخدام معلومات مزيفة والهويات المزيفة في جرائم الانتحال. يسلط الضوء على مؤتمر دولي حول جرائم الحواسيب، مبرزة صعوبة الكشف عن هوية الجانيين ودور الأدلة والذكاء القضائي. يظهر أيضا موقف فرنسا من استخدام لبروتوكول الإنترنت لتحديد عناوين المجرمين الإلكترونيين ويناقش الدور المحتمل للدول في الكشف عن هويات ناشري المحتوى عبر الإنترنت. من خلال كل هذا نتطرق الى تحديات العمل ببروتوكول الإنترنت (TCP/IP) (الفرع الأول)، و موقف المؤتمر الدولي لجرائم الحواسيب من استعمال هذا البروتوكول (الفرع الثاني).

الفرع الأول: تحديات العمل ببروتوكول الإنترنت (TCP/IP)

تظهر تحديات تحديد هوية الجاني في البيئة الرقمية عبر بروتوكول الإنترنت(TCP/IP) ، إذ يُؤكد النص على أن هذا البروتوكول غير موحد على مستوى عالمي ويتغير مع كل

[1] عمر محمد أبو بكر بن يوسف، مذكرات في الإثبات الجنائي عبر الانترنت، بحث مقدم إلى ندوة الدليل الرقمي، بمقر جامعة الدول العربية بالقاهرة، في الفترة الممتدة من 05 إلى 08 مارس 2006، ص ص 01-27 ص 811.

اتصال. تبرز صعوبة تحديد هوية الفاعل، حيث يتعارض كل عنوان IP مع عدة هويات، مما يعزز التعقيد في هذا السياق الرقمي.

تُعقد الأمور أكثر عند استخدام معلومات مزيفة في عناوينIP ، ونُشير إلى أن ذلك يمكن أن يحدث عند استخدام برامج خبيثة تُضيف معلومات كاذبة، مما يجعل من الصعب تحديد هوية الجاني.[1]

نتسلط الضوء أيضا على التحديات في حالات قرصنة عناوين البريد الإلكتروني واستخدامها في جرائم باسم صاحبها. نسلط الضوء على التقنية الخبيثة للصيد (Phishing)، حيث يُشير إلى إغراء الأفراد بعروض مغرية ومزيفة، مما يؤدي إلى سرقة بياناتهم لاستخدامها في جرائم باسم آخر.[2]

الفرع الثاني: موقف المؤتمر الدولي لجرائم الحواسيب من استعمال بروتوكول الإنترنت لتحديد عنوان المجرم الاكتروني

في مؤتمر الدولي لجرائم الحواسيب الذي أقيم في أوسلو بين 29 و 31 مايو 2000، أُثيرت مسألة حيوية تتعلق بالتحقيق في الجرائم الإلكترونية. تم التركيز على التحديات التي تواجه هياكل الإنترنت في تحديد هوية الجناة، رغم وجود وسائل فعّالة لتحديد المكان والأجهزة، مثل عناوينIP ، التي تُستخدم كوسيلة رئيسية لارتكاب هذه الجرائم[3].

وفي هذا السياق، أشار بعض المشاركين في المؤتمر إلى أن قضية عدم الكشف عن هوية الفاعلين وراء الرسائل غير الشرعية هي قضية نسبية. هم يبرزون عدم إمكانية تجهيل شامل في شبكة المعلومات، حيث يترك الجناة آثارًا يمكن للمحققين استخدامها. يتوقف الأمر إلى حد كبير على ذكاء رجال الضبطية القضائية في تحليل الأدلة ورصد الشكوك. وفي حال استخدام الجريمة حاسوبًا شخصيًا، يمكن للمحقق استجواب

---

[1] غنام محمد غنام، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والانترنت و جرائم الاحتيال المنظم باستعمال شبكة الانترنت، طبعة1، دار الفكر والقانون، القاهرة، 2013، ص 220.

[2] HABHAB Mohamad Ahmad, le droit pénal libanais a I Epreuve de la cybercriminalité, thèse de doctorat, soutenu a la Faculté de droit de Université Montpellier, le 10 juillet 2009, p.p 115-116.

[3] موسى مسعود أرحومة، الإشكالات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، بحث مقدم إلى المؤتمر المغاربي الأول حول المعلومات والقانون المنظم من طرف أكاديمية الدراسات العليا، طرابلس، الفترة الممتدة من 28-29/ 10/2009، دون ترقيم الصفحات.

صاحب الحاسوب المشتبه فيه حول تفاصيل استخدامه ومدة استخدامه، ومقارنة هذه المعلومات بتفاصيل الجريمة. يبرز تحديد هوية المستخدمين عبر الإنترنت وتتبع الآثار دورًا حيويًا في الكشف الجنائي.[1]

وفي هذا السياق، فرضت بعض الدول، مثل فرنسا، الكشف عن هويات ناشري محتوى الرسائل والمشتركين في شبكات المعلومات على مزودي خدمات الاتصال والإنترنت. هذه الخطوة تعزز الشفافية وتساعد السلطات القضائية في الكشف عن هويات المجرمين وجمع الأدلة بشكل أفضل.[2]

المبحث الثاني: فرض الجناة لتدابير أمنية

مع التطور المتسارع للتحقيقات في مجال مكافحة الجرائم الإلكترونية، يظهر أمام السلطات القانونية تحديات ضخمة في سبيل الوصول إلى الأدلة الرقمية. يتسلح المجرم الإلكتروني بتقنيات التشفير والشفرات الرياضية المعقدة لتحجيم المعلومات بشكل يفوق الفهم العادي. تبرز تعقيدات تحديد هوية الجاني وتعقيدات التقنيات المستخدمة في فك تشفير هذه البيانات. يتناول الموضوع تأثير استخدام التشفير في حماية الأجهزة ويسلط الضوء على التحديات التي يواجهها المتهمون الذين يواجهون خيارات صعبة، ويعكس صعوبة الكشف عن كلمات السر وحق المتهم في الصمت. تظهر براعة المجرم الإلكتروني في التخطيط والاستفادة من تقنيات الحماية، مؤكدًا على تعقيدات فك تشفير البيانات واستخدام الرياضيات التطبيقية لتحقيق هذا الهدف. يسلط الضوء على أهمية تطوير تفاهم عميق لعلم تحليل الشفرات بهدف تعزيز فعالية التحقيقات في جرائم الأمان السيبراني ومجالات التشفير. نتطرق من خلال هذا المبحث الى تحديات المحققين في فك الشيفرات التقليدية (المطلب الأول)، والى تحديات المحققين في فك الشيفرات الحديثة (المطلب الثاني).

[1] موسى مسعود أرحومة، مرجع سابق، دون ترقيم صفحات.

[2] البربري صالح أحمد، دور الشرطة في مكافحة جرائم الانترنت في إطار اتفاقية بودابست، نشر في 16-1-2019، 10-9-2023، مقال متاح في الموقع www.Arablaw.Com .

المطلب الأول: تحديات المحققين في فك الشيفرات التقليدية

تزايد التحقيقات في مكافحة الجرائم الإلكترونية يكشف عن تحديات في الوصول إلى الأدلة بسبب استخدام المجرمين للتشفير والشفرات الرياضية المعقدة. يسلط الضوء على تعقيدات تحديد هوية الفاعل وصعوبات فك تشفير البيانات، مبرزًا استخدام التشفير لحماية الحاسوب والصعوبات التي تواجه السلطات في كشف كلمات السر. يعكس هذا الموضوع براعة المجرمين الإلكترونيين ويشدد على أهمية تطوير فهم عميق لعلم تحليل الشفرات لتعزيز كفاءة التحقيقات في جرائم الأمان السيبراني والتشفير. نتطرق في هذا المطلب الى الاستراتيجيات الرياضية والجبرية المعقدة لتشفير المعلومات (الفرع الأول)، والى فك تشفير المعلومات من خلال الحصول على مفاتيح التشفير أو تحليل الشيفرات بدون المفاتيح (الفرع الثاني).

الفرع الأول: الاستراتيجيات الرياضية والجبرية المعقدة لتشفير المعلومات

ما قد يعقد مهمة السلطات القانونية في الوصول إلى الدليل. يتسلح المجرم الإلكتروني بالتشفير والشفرات الرياضية المعقدة، حيث يمكنه إخفاء المعلومات المرسلة واستقبالها بطريقة غير قابلة للفهم، ما يترك الباحثين أمام تحديات تقنية كبيرة في فك هذه التشفيرات. وفي حالة حماية حاسوبه، يتعامل المتهم مع خيارين صعبين، إما الكشف عن كلمة السر للسلطات أو حماية محتوى جهازه بحيث يظل غير قابل للوصول. يشير هذا إلى التواجه بتحديات قانونية حينما يرفض المتهم الكشف عن كلمة السر، حيث يحظى بحقه في الصمت ويجعل العملية تعقيدية أمام القانون.[1]

المجرم الإلكتروني يبرع بالتخطيط واستخدام أساليب أمنية لحماية جريمته. يستخدم كلمات مرور ويشفر البيانات بشكل يعيق التحقيقات. حماية حاسوب الجريمة بكلمة السر تضع المُفتش في خيارين، طلب كلمة السر من المتهم أحيانًا بالإفصاح، لكن القانون يحمي حقه في الصمت. فك شيفرة الوصول يواجه الباحث بتحديات تتطلب جهدًا ووقتًا، وغالبًا يحتاج إلى خبرة عالية. يستخدم التشفير لحماية البيانات برموز

[1] الصغير جميل عبد الباقي، أدلة الإثبات الجنائي والتكنولوجية الحديثة، الطبعة1، دار النهضة العربية، القاهرة، 2002، ص115.

رياضية معقدة. هذه التقنيات تعكس ذكاء وتكنولوجيا عالية، مما يعزز التحدي الذي يواجه السلطات في مجال مكافحة جرائم الإنترنت.[1]

الفرع الثاني: فك تشفير المعلومات من خلال الحصول على مفاتيح التشفير أو تحليل الشفرات بدون المفاتيح

المتهم الإلكتروني يستخدم تقنيات تشفير لحماية بياناته وحاسوبه من التحقيقات. يعتمد التشفير على استخدام رموز وإشارات غير تقليدية، مما يجعل البيانات غير قابلة للقراءة للأفراد غير المخولين. يتضمن هذا العملية استخدام خوارزميات رياضية معقدة لتحقيق تأمين فعال. لفك هذا التشفير، يواجه المحققون تحديات، حيث يحتاجون إما للحصول على المفاتيح المستخدمة في التشفير أو لتحليل الشفرات بدون المفاتيح. علم استرجاع النص الواضح بدون معرفة المفاتيح يعتبر أساسيًا في تحليل الشفرات، حيث يعتمد على الرياضيات التطبيقية وفروعها المختلفة. يشمل ذلك نظرية الاحتمالية ونظرية الإعداد والإحصاء والجبر. يكمن في هذا السياق أهمية تطوير الفهم العميق لعلم تحليل الشفرات للتمكن من التحقيق بفعالية في جرائم الأمان السيبراني والتشفير.[2]

عندما يلجأ المجرم الإلكتروني إلى تشفير البيانات في حاسوبه، يتبع استراتيجية تهدف إلى إخفاء هذه البيانات عبر استخدام رموز وإشارات معقدة. في جوهرها، يعكس عملية التشفير محاولة المجرم لحماية البيانات من الوصول غير المصرح به، حيث يتم تحويل هذه البيانات إلى شكل لا يمكن قراءته بسهولة.

لفهم كيفية التعامل مع هذا السيناريو، يجد المحقق نفسه في موقف يتطلب إما الحصول على مفاتيح التشفير من المجرم نفسه، أو بذل مجهودات لتحليل الشفرات بدونها. في هذا السياق، يتجه الاهتمام نحو علم استرجاع النصوص الواضحة بدون

[1] عبد الحميد عبد المطلب ممدوح، جرائم استخدام شبكة المعلومات العالمية، بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون الإمارات العربية المتحدة ، 2000، ص ص 24 وما بعدها.

[2] إسماعيل عبد النبي شاهين، أمن المعلومات في الانترنت، بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون الإمارات العربية المتحدة، 2000، ص 11.

مفاتيح، حيث يتطلب ذلك إلمامًا عميقًا بالرياضيات التطبيقية وفهمًا شاملاً لنظريات مثل نظرية الاحتمال ونظرية الإعداد والإحصاء والجبر.[1]

تلك المعرفة العميقة تسهم في تمكين المحققين من التفاعل بشكل فعّال مع التحديات التي يفرضها تشفير البيانات، مما يعزز قدرتهم على الكشف عن الحقائق في سياق التحقيقات الإلكترونية.

المطلب الثاني: تحديات المحققين في فك الشيفرات الحديثة

تقنية إخفاء المعلومات (Steganography) تستخدمها المجرمين الإلكترونيين لتضليل آثار جرائمهم، حيث يخفون بيانات هامة داخل بيانات أخرى بشكل غير ملحوظ، سواء في ملفات مصورة أو صوتية أو حتى بيانات تنفيذية لبرامج الحاسوب. يظهر صراعًا بين حماية البيانات وضمان الأمان السيبراني، مع تبني بعض الدول لسياسات تنظيمية صارمة لاستخدام التشفير بهدف تحقيق توازن بين الأمان الوطني وحقوق الأفراد. لهذا سنتطرق في هذا المطلب الى تقنية اخفاء المعلومات (Steganography) (الفرع الأول)، والى الموازنة بين فك الشيفرات وضمان الأمان وبين الحفاظ على حقوق وحريات الأفراد (الفرع الثاني).

الفرع الأول: تقنية اخفاء المعلومات (Steganography)

تقنية إخفاء المعلومات (Steganography) تشكل وسيلة حديثة للمجرم الإلكتروني لتضليل وتخفي آثار جريمته. في هذه التقنية، يقوم المجرم بتضمين بيانات هامة داخل بيانات أخرى بطريقة تجعلها غير ملحوظة للعيان البشري وتستخدم لها برامج التحليل للكشف عنها. يمكن أن تكون هذه البيانات المخفية مدمجة في ملفات مصورة، صوتية، فيلمية، أو حتى في بيانات تنفيذية لبرامج الحاسوب. في مثال عملي، يمكن للمجرم إخفاء بيانات داخل صورة دون أن يكون للعيان البشري أي علم بوجود تغيير. يمكن أيضًا استغلال المساحة الهادئة (Slack) في القرص الصلب، حيث يمكن للمجرم تخزين بياناته في هذه المساحة المخصصة عادة لأنظمة التشغيل دون أن يشعر المستخدم العادي. عملية الكشف عن البيانات المخفية (Steganalysis) تعتمد على تحليل عميق للصور أو البيانات للكشف عن أي تغييرات غير مرئية. يتطلب هذا التحليل فهمًا عميقًا

[1] محمد حسام محمود لطفي، الجرائم التي تقع على الحاسبات أو بواسطتها، بحث مقدم الى المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، 1993، ص 496.

للرياضيات التطبيقية وفروعها المتقدمة مثل نظرية الاحتمال ونظرية الإعداد والإحصاء والجبر. هذه العملية تعتبر معقدة وتتطلب خبرة متقدمة، وهي خطوة أساسية لرجال التحقيق للوصول إلى أدلة قوية تستخدم ضد المتهم.[1]

الفرع الثاني: الموازنة بين فك الشيفرات وضمان الأمان وبين الحفاظ على حقوق وحريات الأفراد

في ظل التطور التكنولوجي المتسارع، يبرز الصراع بين الحاجة لحماية البيانات وضمان الأمان السيبراني، وبين حقوق الأفراد في الحفاظ على خصوصيتهم. بعض الدول تتبنى سياسات تشدد فيها على تنظيم استخدام تقنيات التشفير، مثل فرنسا التي فرضت قوانين تتطلب الحصول على تراخيص لاستخدام التشفير وتودع مفاتيح التشفير لدى الجهيئات معينة. هذا النهج يعكس توازناً دقيقاً بين الأمان الوطني وحقوق الأفراد، إذ يسعى إلى تفادي إساءة استخدام تقنيات التشفير في الأنشطة الإجرامية أو الإرهابية، مع الحفاظ على حقوق الأفراد في استخدام هذه التقنيات للحفاظ على خصوصيتهم. وفي هذا السياق، تمنع تشريعات بعض الدول اللجوء إلى تقنيات التشفير بدون ترخيص، وتفرض قيوداً صارمة تتعلق بالحصول على تصاريح مسبقة. على سبيل المثال، في فرنسا، يتعين على من يقوم بتشفير بياناته الحصول على ترخيص من الجهات المختصة، وكذلك إيداع مفاتيح التشفير لديها. وأي انتهاك لهذه التزامات يُعتبر جريمة تخضع للعقوبات القانونية.[2]

هذا التنظيم يسعى للحفاظ على التوازن بين استخدام فعّال لتقنيات التشفير للحماية من التهديدات السيبرانية، وحقوق الأفراد في حماية خصوصيتهم وحرياتهم الشخصية.

[1] مكاوي مراد عبد الرحمان، مرجع سابق، ص 43.

[2] HABHAB Mohamed Ahmad, op.cit. p 120.

خاتمة:

الاجابة عن التساؤلات:

اجابة على التساؤلات الموجودة في المقدمة يمكن تحسين عمليات تحديد عناوين وهويات المجرمين الالكترونيين من خلال التركيز على تطوير تقنيات التحليل الرقمي واستخدام الذكاء الاصطناعي لتعزيز دقة التحليل. كما يتطلب الأمر تعزيز التعاون الدولي لتبادل المعلومات وتطوير استراتيجيات مشتركة. يمكن تعزيز الكفاءة بتبني تقنيات متقدمة وتحسين تدريب الكوادر الأمنية. يجب أيضًا التركيز على تطوير أساليب لكسر تشفير البيانات المستخدمة بواسطة المجرمين. إصدار قوانين صارمة وفعّالة، وتعزيز الأمان السيبراني لحماية الأنظمة الحيوية، يشكل جزءًا أساسيًا من تعزيز التصدي لتحديات الجرائم الإلكترونية.

النتائج:

صعوبة تحديد مكان جهاز الحاسوب: تعتبر صعوبة تحديد مكان جهاز الحاسوب مصدر التحدي للتحقيق في الجرائم الإلكترونية.

التقنيات الحالية قد تكون غير كافية: الاعتماد على تقنيات البصمات المعاصرة قد لا تكون كافية للتعامل مع التحديات المتزايدة لتمويه هوية الجناة الرقميين.

تحديات في الكشف عن مصدر الجريمة: التقنية المعتمدة على نظام (TCP/IP) قد توفر عنوان رقمي للحاسوب فقط (adresse IP)، مما يجعلها غير كافية لتحديد مصدر الجريمة بشكل دقيق.

عدم توثيق الهوية بشكل كافي: العنوان الرقمي للحاسوب قد يكون مسروقًا أو يتم استخدامه احتيالًا، مما يجعله غير كافٍ لإسناد الفعل الإجرامي إلى صاحب الحاسوب.

تغير العناوين الرقمية بشكل دائم: نظام (TCP/IP) يعرض صعوبة في تحديد الجهاز المرتكب للجريمة الإلكترونية بشكل دائم، حيث يتغير العنوان الرقمي مع كل اتصال بشبكة الإنترنت.

الصعوبات في التعامل مع عناوين (IP) الغير حقيقية: التلاعب بمعلومات العناوين (IP) واستخدامها بشكل زائف يزيد من صعوبة تحديد هوية صاحب الحاسوب وتصعيد الجرائم الإلكترونية.

التخطيط والذكاء الفني: مهارات التخطيط والذكاء الفني للمجرم الإلكتروني يصعب على السلطات القانونية التحقق من هويته والوصول إلى دلائل الجريمة.

تأمين الجريمة بطرق فنية: استخدام التشفير وكلمات المرور يزيد من تأمين الجرائم الإلكترونية ويجعل صعباً على رجال الاستدلال الوصول إلى المعلومات.

حماية بيانات الحاسوب: تكون كلمات السر وتشفير البيانات تحديًا إضافيًا لرجال التحقيق للوصول إلى محتوى الحاسوب المستخدم في ارتكاب الجريمة.

رفض التعاون: رفض المتهم الكشف عن كلمة السر يعتبر حقًا قانونيًا، مما يجعل التعاون مع رجال التحقيق أكثر صعوبة.

تشفير البيانات: استخدام التشفير يعيق رجال التحقيق من الوصول إلى المعلومات المرتبطة بالجريمة، حيث يصعب فك شيفرة البيانات بدون المفاتيح الصحيحة.

صعوبة الاستجواب بدون مفاتيح الشفرة: رفض المتهم الكشف عن مفاتيح التشفير يمثل تحديًا إضافيًا، حيث قد يكون من الصعب إجباره على التعاون.

الحاجة إلى تخصص رياضي متقدم: فك تشفير البيانات يتطلب خبرة رياضية متقدمة وفهمًا عميقًا في ميدان تحليل الشفرات.

استعمال فيروسات الحماية: استخدام الفيروسات للحماية يضع عائقًا آخرًا أمام رجال التحقيق، حيث يتم تلفيق حماية الحاسوب بطرق قد تضر بجهود الاستدلال.

تقنية إخفاء المعلومات: تقنية الاختباء (Steganography) تسهم في إخفاء البيانات وتعقيد مهمة رجال التحقيق في اكتشاف وفحص الأدلة.

تعقيد التحليل العلمي: تحليل البيانات المخفية يتطلب خبرة علمية ورياضية معقدة، مما يزيد من تعقيد عمليات التحقيق.

التحديات في اكتشاف المساحة الهادئة: استخدام المساحة الهادئة (Slack) لتخزين المعلومات يعزز صعوبة اكتشاف البيانات المخفية.

الاقتراحات:

تطوير تقنيات جديدة: الاستثمار في البحث وتطوير تقنيات جديدة لتحديد مكان جهاز الحاسوب بشكل أفضل وأكثر دقة.

تعزيز التعاون الدولي: تعزيز التعاون الدولي في تبادل المعلومات وتقنيات التحقيق لمكافحة الجرائم الإلكترونية عبر الحدود.

تعزيز التشريعات الرقمية: تحديث التشريعات لتكون متواكبة مع التطورات التكنولوجية وتمكين السلطات من مواجهة التحديات القانونية في التحقيق في الجرائم الإلكترونية.

تطوير الوعي الرقمي: توعية المستخدمين بأهمية الأمان الرقمي وتبني عادات استخدام آمنة للحد من انتشار الجرائم الإلكترونية.

تعزيز التدريب: تعزيز تدريب الكوادر القانونية والتحقيق على أحدث التقنيات والأساليب في مجال مكافحة الجرائم الإلكترونية.

تشديد التدابير الأمنية: تعزيز التدابير الأمنية لمنع سرقة العناوين الرقمية وضمان استخدامها بشكل صحيح.

توعية مقدمي الخدمة: توجيه جهات مقدمي الخدمة لتحديد شخصية المشترك وتوثيق الهوية قبل توصيل الأسماء المجهولة.

تحسين تقنيات تحديد الهوية: العمل على تحسين التقنيات التي تسمح بتحديد هوية صاحب الحاسوب بشكل دائم حتى في حالة تغيير العنوان الرقمي.

توحيد البروتوكولات: العمل على توحيد وتطوير بروتوكولات الإنترنت لتكون أكثر استقرارًا وتوحيدًا على مستوى عالمي.

تشديد الأمان الرقمي: تعزيز التدابير الأمنية لتجنب تزوير عناوين (IP) والتحقق من صحتها بشكل دوري.

تحسين تشريعات مكافحة الجرائم الإلكترونية: تحسين التشريعات لمواجهة تحديات استخدام العناوين (IP) بشكل غير قانوني وتعزيز العقوبات ضد الجرائم الإلكترونية.

تعزيز فعالية التحقيق: تعزيز فعالية تقنيات تحديد الهوية وتتبع الآثار عبر الإنترنت لتحديد هوية المستخدمين بشكل أدق.

تبني أساليب متقدمة لتحليل الآثار: استخدام أساليب متقدمة لتحليل الآثار ومعلومات الشبكة لتسهيل تحديد المجرمين والوصول إلى الأدلة.

توجيه الضوء على فحص الآثار: التركيز على تدريب رجال التحقيق لفحص الآثار التي يتركها المجرمون عبر الإنترنت والاستناد إلى الشفافية لتحقيق نجاعة أكبر.

تطوير تقنيات الاستدلال: تطوير تقنيات استدلال جديدة للتعامل مع تشفير البيانات وحماية الحاسوب لتمكين رجال التحقيق من الوصول إلى المعلومات بشكل أفضل.

تطوير تقنيات فك التشفير: الاستثمار في البحث والتطوير لتطوير تقنيات جديدة لفك التشفير أو تسهيل هذه العملية.

تطوير أدوات للتحليل الأوتوماتيكي: استثمار في تطوير أدوات تحليل أوتوماتيكية لاكتشاف وفحص البيانات المخفية، مما يقلل من التأثير الضار لتلك التقنية.

قائمة المراجع باللغة العربية:

أولا/الكتب:

أ- الصغير جميل عبد الباقي، أدلة الإثبات الجنائي والتكنولوجية الحديثة، الطبعة1، دار النهضة العربية، القاهرة، 2002.

ب- غنام محمد غنام، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والانترنت و جرائم الاحتيال المنظم باستعمال شبكة الانترنت، طبعة1، دار الفكر والقانون، القاهرة، 2013، ص 220.

ثانيا/المقالات في الملتقيات والندوات:

أ- إسماعيل عبد النبي شاهين، أمن المعلومات في الانترنت، بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون الإمارات العربية المتحدة، 2000، ص 11.

ب- راسل تاينر، أهمية التعاون الدولي في منع جرائم الانترنت، بحث مقدم إلى الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، الجارية بالمملكة المغربية، في الفترة 19 و 20 جوان 2007، ص ص 113-114.

ج- محمد حسام محمود لطفي، الجرائم التي تقع على الحاسبات أو بواسطتها، بحث مقدم الى المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، 1993، ص 496.

د- موسى مسعود أرحومة، الإشكالات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، بحث مقدم إلى المؤتمر المغاربي الأول حول المعلومات والقانون المنظم من طرف أكاديمية الدراسات العليا، طرابلس، الفترة الممتدة من 28/10/2009/ 29-، دون ترقيم الصفحات

هـ- عبد الحميد عبد المطلب ممدوح، جرائم استخدام شبكة المعلومات العالمية، بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون الإمارات العربية المتحدة ، 2000، ص ص 24 وما بعدها.

و- عمر محمد أبو بكر بن يوسف، مذكرات في الإثبات الجنائي عبر الانترنت، بحث مقدم إلى ندوة الدليل الرقمي، بمقر جامعة الدول العربية بالقاهرة، في الفترة الممتدة من 05 إلى 08 مارس 2006، ص ص 01-27 ص 811.

ثالثا/المقالات في مو اقع الانترنت:

أ- البربري صالح أحمد، دور الشرطة في مكافحة جرائم الانترنت في إطار اتفاقية بودابست، نشر في 16-1-2019، 10-9-2023، مقال متاح في الموقع www.Arablaw.Com .

ب- عبد الحميد عبد المطلب، استخدام برتوكول (TCP/IP) في بحث و تحقيق الجرائم على الكمبيوتر، 15-1-2019، 1-12-2023، منشور على الموقع الالكتروني www.arablaw.info.com.

قائمةالمراجع باللغة الأجنبية:

HABHAB Mohamad Ahmad, le droit pénal libanais a I Epreuve de la cybercriminalité, thèse de doctorat, soutenu a la Faculté de droit de Université Montpellier, le 10 juillet 2009, p.p 115-116.

T.G.I. novembre, 1998, disponible a l'adresse suivant; http://www.legalis.jnet.decision/illicite -divers/correct-Paris-1998-htm .