منهج وقواعد النقد الدبلوماتي الرقمي في عملية الإثبات الجنائي للوثائق (الأدلة) الرقمية: دراسة تطبيقية من واقع الجرائم المعلوماتية

د . حسناء علي علي عبد الغني

قسم الوثائق والمكتبات والمعلومات

كلية الدراسات الإنسانية

جامعة الأزهر، القاهرة، مصر

Hasnaa.study@gmail.com

مستخلص

هدفت هذه الدراسة إلى التأكيد على دور علم الوثائق (الدبلوماتيك) في عملية الإثبات الجنائي الرقمي، وأهمية دورالنقد الدبلوماتي الرقمي وتطبيقه على الوثائق الرقمية بهدف ضرورة التأكيد على صحة إجراءات الحصول على الوثائق (الأدلة) الرقمية، وكيفية الوصول إلى صدق وصحة وتكامل الوثائق وعدم تعرضها للتلف أو التغيير أو التبديل أو التحريف وصحة نسبتها إلى الجاني على نحو يجعل القاضي يستند إليها في تكوين عقيدته وبناء حكمه. وقد تناولت الدراسة تطبيق منهج وقواعد النقد الدبلوماتي الرقمي على نماذج من الوثائق (الأدلة) الرقمية للجرائم المعلوماتية في مصر. وتوصلت الدراسة إلى أن أوجه التطابق بين منهج علم الدبلوماتيك الرقمي ومنهج علم الإثبات الجنائي الرقمي تتمثل في تقييم أصالة وتحديد سياق ومصدر وعلاقات ومعنى الوثائق (الأدلة) الرقمية.

الكلمات المفتاحية: الوثائق الرقمية ؛ علم الوثائق (الدبلوماتيك) الرقمي ؛ علم الإثبات الجنائي الرقمي؛ الجريمة المعلوماتية.

تاريخ استلام البحث: 2022/10/3 **تاريخ إجازة البحث: 2022/10/18**

المقدمه

علم الوثائق (الدبلوماتيك) أحد العلوم التي ظهرت بشكلٍ تلقائي عملي، ثم تطورت إلى وضع القواعد التي يمكن من خلالها الحكم على وثيقة ما بالصحة أوالتزوير. وكان "مابيون" أول من وضع مجموعة من القواعد، التي تكشف عند تطبيقها صحة الوثائق أو تكشف ما مسها من تزوير.

وقد تبنى المؤرخون في القرن التاسع عشر هذا العلم كأداة لنقد الوثائق من أجل تقييم مصداقية وثائق العصور الوسطى كالوثائق التاريخية. أي أن تحديد مدى صحة الوثائق الفردية في العصور الوسطى كان هو السبب الأصلي لنشأة علم الدبلوماتيك في القرن السابع عشر.

ولأن التغيير سمة الحياة، والعلم مظهر من مظاهر الحياة التي تتضح فيه هذه السمة بشكلٍ جلي، فإن علم الوثائق (الدبلوماتيك) مثله مثل بقية العلوم التي تصدق عليه هذه الحقيقة، فهو علم يتغير ويتطور كذلك في منهجه وهدفه تبعاً للظروف والبيئة المحيطة والزمان والمكان. وقد تبنت لوسيانا دورانتي رحلة تطوير علم الوثائق (الدبلوماتيك)، حيث قدمت أفكارها الجديدة في المجتمع الأرشيفي بشمال أمريكا، وكونت فريق عمل نشط بجامعة كلومبيا البريطانية كمشروع بحثي مهم لهذا الغرض، ألا وهو تطوير علم الوثائق (الدبلوماتيك) بمفهوم عصري لمواكبة التطورات التكنولوجية الحديثة، والتي نتج عنها أنواعاً وأشكالاً جديدة من الوثائق الإلكترونية التي نشأت وظهرت معها مشكلة عدم الثقة بها، حيث فرضت البيئة التكنولوجية الحديثة تحديات كثيرة أمام بناء الثقة في هذه الوثائق، وأصبحت الوثائق الرقمية مشكوك في صحتها، وبحاجة إلى من يبرهن على صحتها والحفاظ عليها صحيحة دائما، الأمر الذي جعل علم الوثائق (الدبلوماتيك) يعود إلى الهدف الأصلي الذي أُنشئ من أجله وهو إثبات صحة الوثائق أو زيفها، حيث يمكن من خلال علم الوثائق (الدبلوماتيك) الرقمي التعرف على الوثائق (الأدلة) الرقمية وفهم طبيعتها وخصائصها وتوابعها القانونية.

ولا شك أنَ الفهم العميق للوثائق الرقمية المكتسب من خلال تحليل علم الدبلوماتيك الرقمي سيكون مفيدا لخبراء الإثبات الجنائي الرقمي، الذين تتمثل مهمتهم الأساسية في الحصول على أدلة من البيئة الرقمية دون التدخل فيها، أي الحفاظ على هوية سليمة للأدلة وحماية سلامتها، وكذلك سلامة النُسخ التي يقدمونها.

وتجدر الإشـــارة إلى أن التحديات التي طرحتها البيئة التكنولوجية الحديثة أمام بناء الثقة في الوثائق الرقمية قد مهدت الطريق لمزيد من المشـروعات البحثية، مثل مشـروع الإثبات الجنـائي للوثـائق الرقميـة DRF، حيـث قـام فريق مكون من مختصـــين في الـدبلومـاتيـك وعلم الأرشـيف وعلم المعلومات وقانون الأدلة والإثبات الجنائي الرقمي, بتطبيق برنامج بحثي غرضـه تطوير مجال علمي جديد متعدد التخصـــصـــات يطلق عليه "الإثبات الجنائي للوثائق الرقمية Digital Records Forensics (DRF)", وذلـك من خلال دمج مفـاهيم ومنـاهج جميع العلوم ســـابقة الذكر. تناول هذا المشـــروع البحثي بعض التحديات التي تطرحها التكنولوجيا الرقمية لإدارة الوثائق والأرشـيف والمهن القانونية، **ومن بين هذه التحديات**: تحديد الوثائق في الأنظمة الرقمية المعقدة وتحديد أصالتها.

ومن هنا يمكن القول أن علم الوثائق (الـدبلوماتيك) قـد خطا خطواتٍ واســـعـة نحو اسـتعادة الهدف الأصلي من نشـأته، فلم يعد تخصصاً علمياً يقوم على تجميع وتحليل البيانات فقط، أي أنه لم يعُد الشـــق التحليلي في المنهج التاريخي بل أصـــبح منهجاً بحثياً يســـتخدمه العاملون في مجال الوثائق والأرشيف والقانون وتكنولوجيا الحاسبات والإثبات الجنائي الرقمي. وأصـــبح الدبلوماتيون يعملون جنباً إلى جنب مع مهندســـي الحاســـب الآلي والخبراء القانونيين لتحليل جميع المكونات التكنولوجية لكل نظام ووظيفته المحددة، ودراســـة أثر التغيير الذي تتعرض لـه مكونـات الشـــكل المـادي والفكري للوثـائق المنتجـة أو المتســـلمـة أو المحتفظ بهـا في النظام.

ومن هنـا تظهر أهميـة علم الوثـائق (الـدبلومـاتيـك) بـالنســـبـة لعلم الإثبـات الجنـائي الرقمي، حيـث أصـــبح علم الإثبـات الجنـائي الرقمي في حـاجـة إلى علم الوثـائق (الـدبلومـاتيـك) لإستخدام منهجه في التعرف على مكونات الوثائق الرقمية وكيفية نقدها.

مشكلة الدراسة وأهميتها :

تعتبر مســـألـة التعرف على الوثـائق (الأدلـة) من بين جميع المخرجـات الرقميـة التي تنتجها الأنظمة التفاعلية المعقدة, وتحديد مدى صـحتها, من أصـعب القضـايا التي تفرضـها التكنولوجيا الرقمية على مجالات إنفاذ القانون, وإدارة الوثائق, ومهنة الأرشـفة ومهنة القانون. كما أن فهم هذه الوثائق (الأدلة) وتتبع مصـدرها وتقييم مدى صـحتها يُثير مشـكلات كثيرة في الإثبات الجنائي الرقمي نظراً للطبيعة غير المادية للوثائق (الأدلة) الرقمية، حيث تتميز هذه

الوثائق (الأدلة) بطبيعة خاصة تميزها عن غيرها من الوثائق (الأدلة) التقليدية. فتتميز بأنها وثائق (أدلة) تقنية، يسهل إخفاؤها أو محوها، كما أنه يصعب فهمها نظراً لقلة الآثار المادية المتخلفة عن هذه الجرائم، وإمكانية التلاعب في البيانات والبرامج من أماكن بعيدة أو محوها من قبل الجاني، بالإضافة إلى إستخدام بعض البرامج الإلكترونية التي تؤدي إلى إزالة الآثار والأدلة التي تثبت وقوع الجريمة ونسبتها إلى فاعل معين مما يجعل عمل الجهات المختصة بالتحقيق في الجرائم المعلوماتية أكثر صعوبة لعدم قدرتهم على فك رموز الكثير من المسائل الفنية الدقيقة، الأمر الذي يتطلب ضرورة الإحاطة بمكونات الحاسب الآلي وبنظام المعالجة الآلية للبيانات والشبكات وبطرق الدخول إليها، وكل ما يتعلق بهذه الجرائم من تقنياتٍ وحداثة، وهذا يتطلب جُهداً فنياً فضلاً عن الجُهد القانوني، كما يتطلب الإستعانة بعلم الوثائق (الدبلوماتيك) الرقمي في التعرف على الوثائق (الأدلة) الرقمية وفهم طبيعتها وخصائصها وتقييم صحتها. وقد كتب الدبلوماتيون المعاصرون عن استخدام علم الوثائق (الدبلوماتيك) في الإثبات الجنائي الرقمي، وكذلك فعل رجال الأدلة الجنائية الرقمية، حيث يمكن من خلال الدبلوماتيك الرقمي وضع منهج لتحليل هوية وتكامل الوثائق في النظم الإلكترونية وتقييم صحتها ومصداقيتها وتتبع نشأتها ومصدرها. كما يمكن من خلاله التعرف على مكونات الوثائق الرقمية وكيفية نقدها. ومن هنا يمكن القول، أنه برزت أهمية علم الوثائق (الدبلوماتيك) الرقمي ودوره في إثبات صحة الوثائق مع ظهور علم الإثبات الجنائي الرقمي.

وقد وقع الإختيار لدراسة هذا الموضوع لأهميته بالنسبة لعلم الوثائق (الدبلوماتيك)، بالإضافة إلى إبراز الدور الجديد للوثائقيين في مجال الإثبات الجنائي الرقمي، حيث أصبح مسئولو الفحص الجنائي للوثائق، يلجأون إلى علم الوثائق (الدبلوماتيك) ويستخدمون منهجيته لإثبات صحة الوثيقة أو زيفها.

أهداف الدراسة :

تسعى هذه الدراسة إلى تحقيق هدف رئيس وهو التأكيد على دور علم الوثائق (الدبلوماتيك) في عملية الإثبات الجنائي، وأهمية دورالنقد الدبلوماتي الرقمي وتطبيقه على الوثائق الرقمية بهدف ضرورة التأكيد على صحة إجراءات الحصول على الوثائق (الأدلة) الرقمية، وكيفية الوصول إلى صدق وصحة وتكامل الوثائق وعدم تعرضها للتلف أو التغيير أو

التبديل أو التحريف وصحة نسبتها إلى الجاني على نحو يجعل القاضي يستند إليها في تكوين عقيدته وبناء حكمه. وفي إطار هذا الهدف يتم القيام بالآتي :

1 – إبراز الدور الجديد للدبلوماتيك الرقمي في مجال الإثبات الجنائي الرقمي .

2 – توضيح العلاقة بين علم الوثائق (الدبلوماتيك) وعلم الإثبات الجنائي الرقمي .

3 – دراسة المشروع البحثي للإثبات الجنائي للوثائق الرقمية (DRF).

4 – شرح منهج وقواعد النقد الدبلوماتي الرقمي ومنهج وقواعد علم الإثبات الجنائي الرقمي.

5- تطبيق منهج وقواعد النقد الدبلوماتي الرقمي على نماذج من الوثائق (الأدلة) الرقمية للجرائم المعلوماتية.

تساؤلات الدراسة :

في ضوء الأهداف السابقة تحاول الدراسة الإجابة على التساؤلات الآتية :

1 – ما الدور الذي يقوم به علم الوثائق (الدبلوماتيك) الرقمي في مجال الإثبات الجنائي الرقمي؟

2 – ما العلاقة بين علم الوثائق (الدبلوماتيك) وعلم الإثبات الجنائي الرقمي؟

3 – ما الهدف من المشروع البحثي للإثبات الجنائي للوثائق الرقمية (DRF)، ومنهجه؟

4 – ما الفرق بين منهج وقواعد النقد الدبلوماتي الرقمي ومنهج وقواعد علم الإثبات الجنائي الرقمي؟

5 – ما مدى إمكانية تطبيق منهج وقواعد النقد الدبلوماتي الرقمي على نماذج من الوثائق (الأدلة) الرقمية للجرائم المعلوماتية؟

حدود الدراسة :

الحدود الموضوعية :

يقتصر النطاق الموضوعي لهذه الدراسة على توضيح العلاقة بين علم الوثائق (الدبلوماتيك) وعلم الإثبات الجنائي الرقمي، وإيضاح الدور الجديد للدبلوماتيك الرقمي في مجال الإثبات الجنائي الرقمي، بالإضافة إلى شرح منهج وقواعد النقد الدبلوماتي الرقمي في عملية الإثبات الجنائي الرقمي وتطبيقه على نماذج من الوثائق (الأدلة) الرقمية للجرائم المعلوماتية.

الحدود المكانية :

تتمثل الحدود المكانية في هذه الدراسة في تطبيق منهج وقواعد النقد الدبلوماتي الرقمي على نماذج من الوثائق (الأدلة) الرقمية للجرائم المعلوماتية المنتشرة داخل جمهورية مصر العربية.

وقد اعتمدت هذه الدراسة على منهجين:

الأول: المنهج الوصفي التحليلي، لرصد وتجميع وتحليل البيانات والمعلومات حول عملية الإثبات الجنائي للأدلة الجنائية الرقمية، حيث يقوم المنهج الوصفي التحليلي على رصد ومتابعة دقيقة لظاهرة ما.

الثاني: المنهج المقارن، حيث استخدمت الباحثة المنهج المقارن في المقارنة بين منهج وقواعد النقد الدبلوماتي الرقمي ومنهج وقواعد علم الإثبات الجنائي الرقمي وإبراز أوجه الشبه والاختلاف بينهما.

الدراسات السابقة :

أولاً: الدراسات العربية

من خلال البحث في قواعد البيانات وتتبع الإنتاج الفكري المتعلق بموضوع الدراسة تبين أنه لا توجد دراسات وثائقية عربية تناولت موضوع الدراسة، ولكن توجد بعض الدراسات التي أشارت إلى العلاقة بين علم الدبلوماتيك الرقمي وعلم الإثبات الجنائي، بالإضافة إلى بعض الدراسات التي تناولت عملية الإثبات الجنائي في مجال القانون.

وقد تم تقسيم الدراسات العربية التي أشارت إلى موضوع الدراسة إلى محورين:

المحور الأول : الدراسات التي أشارت إلى الصلة بين الدبلوماتيك الرقمي والإثبات الجنائي

1 - **دينا محمود عبد اللطيف محمد** . (2017). الإتجاهات الحديثة في علم الدبلوماتيك (الوثائق) ومجالات دراسته : دراسة تطبيقية على الوثائق العربية. "أطروحة دكتوراه"، جامعة الأزهر.

أشارت هذه الدراسة إلى العلاقة بين علم الدبلوماتيك (الوثائق) وعلم الإثبات الجنائي الرقمي.

2 - **حســـناء على على عبد الغني**. (2018). المعيار الدولي أيزو 17068 / 2012 موثوقية الطرف الثـالـث لتـأمين الوثـائق الرقميـة : دراســـة تحليليـة وتطبيقيـة للمعيـار في مصـــر. "أطروحـة ماجستير"، جامعة الأزهر.

تناولت هذه الدراســـة توضـــيح مفهوم الإثبات الجنائي الرقمي ودوره في إثبات الثقة للوثائق الرقمية.

المحور الثاني : الدراسات التي أشارت إلى موضوع الدراسة من خلال الشق القانوني

1 - **محمد عبيد ســـيف ســـعيد المســـماري. (2007).** الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية: دراسة تطبيقية مقارنة . بحث مقدم في المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، الرياض : جامعة نايف العربية للعلوم الأمنية.

يقدم هذا البحث دراسة نظرية وعملية عن الإثبات الجنائي للجرائم المعلوماتية، من الجانب القانوني والجانب العلمي الفني الشرعي.

2 - **توفيق عبدالله أحمد الخشـــاشـــنة. (2016).** معاينة مســـرح الجريمة من خلال شـــبكة المعلومات الدولية. "أطروحة دكتوراه"، جامعة عين شمس.

ركزت هذه الدراســـة على المعاينة الإلكترونية كأحد الجوانب الإجرائية الجنائية في التحقيق، كما وضـحت العلاقة بين الجرائم الإلكترونية والدليل الرقمي المسـتخرج من أجهزة الحاسـب، مما يمكن أجهزة التحقيق من التعامل مع الدليل الرقمي لبناء دليل جنائي له حُجية أمام الجهات القضائية المختصة.

3 - **محمود عبد الغني فريد جاد المولى**. (2016). دور الدليل الإلكتروني في الإثبات الجنائي : دراسـة مقارنة بين القانون المصـري والقانونين الأمريكي والفرنسـي. "أطروحة دكتوراه"، جامعة بنها.

عرضـت هذه الدراسـة وجهة النظر التشـريعية في القوانين المقارنة بشـأن إجراءات الحصـول على الأدلة الإلكترونية، وكذلك قبولها في ضـوء النظم الجنائية المختلفة، وكيفية التعامل معها والتأكد من مشـروعية وسـيلة الحصـول عليها، مع مقارنة ذلك بالوضـع التشـريعي القائم في النظام القانوني المصـري للوقوف على أوجه القصـور أو الخلل في التشـريع المصـري بشأن التعامل مع الأدلة الإلكترونية وإقرارها .

ثانياً : الدراسات الأجنبية

1 - Duranti, L. (2009). From digital diplomatics to digital records forensics. *Archivaria*, *68*, 39-66.

تناولت هذه الدراسة المفاهيم الأساسية لدبلوماتيك الوثائق الرقمية، ومقارنتها بالمفاهيم المستخدمة في علم الإثبات الجنائي للوثائق الرقمية .

2 - Duranti, L., & Endicott-Popovsky, B. (2010). Digital Records Forensics: A New Science and Academic Program for Forensic Readiness. Journal of Digital Forensics, Security and Law,5(2), 45–62.

يتناول هذا المقال برنامج بحثي يتم في جامعة كولومبيا البريطانية في كندا، ويهدف إلى تطوير علم جديد متعدد التخصصات يحقق التكامل بين علم الإثبات الجنائي الرقمي، وعلم الوثائق (الدبلوماتيك)، وعلم الأرشيف، وعلم المعلومات، وعلم القانون .

3 - Agarwal, A., Gupta, M., Gupta, S., & Gupta, S. C. (2011). Systematic digital forensic investigation model. *International Journal of Computer Science and Security (IJCSS)*, *5*(1), 118-131.

يحاول هذا المقال الكشف عن تطور نموذج الإثبات الجنائي الرقمي، حيث يقارن بين منهجيات الإثبات الجنائي الرقمي، ويقترح في النهاية نموذجاً منهجياً لإجراء الفحص الجنائي الرقمي .

4 - Duranti, L., & Rogers, C.(2012). Trust in digital records: An increasingly cloudy legal area . Computer law & Security review 28 , pp. 522 – 531.

يهدف هذا المقال إلى تقديم أطر لمفاهيم الثقة في الوثائق والبيانات التي تم تطويرها في سياق علم الأرشيف والفحص الجنائى للوثائق الرقمية, واستكشاف الإطار القانوني العام الذي يتم في إطاره اختبار قضايا الثقة في الأدلة الوثائقية .

وبناءً على ما سبق يتبين أن الدراسة الحالية تختلف عن الدراسات السابقة كما تقوم باستكمالها، في أنها ستقوم بشرح الدور الجديد للدبلوماتيك الرقمي في مجال الإثبات الجنائي للوثائق أو الأدلة الرقمية، لا سيما وأن هذا الدور سوف يفتح مجالاً جديداً للدبلوماتيين (الوثائقيين) للعمل في مجال خبراء التحقيق الجنائي. كما تقوم هذه الدراسة بالتطبيقعلى

نماذج من الوثائق (الأدلة) الرقمية للجرائم المعلوماتية داخل جمهورية مصر العربية، مما يُعطيها بُعداً تطبيقياً عملياً.

تمهيد

إن المنهج الوثائقي ذو أهمية بالغة في فحص أحداث الماضي، والحاضر، ولقد تجلت أهميته ودوره في إثبات صحة الوثائق مع ظهور علم الإثبات الجنائي الرقمي، فلم يعد علم الوثائق تخصصاً علمياً يقوم على تجميع وتحليل البيانات فقط، أي أنه لم يعُد الشق التحليلي في المنهج التاريخي[1] بل أصبح منهجاً بحثياً يستخدمه العاملون في مجال الوثائق والأرشيف والقانون وتكنولوجيا الحاسبات والإثبات الجنائي الرقمي أيضاً[2].

لقد شكل علم الدبلوماتيك والمناهج التي يتبعها جزءاً كبيراً من قواعد قبول الأدلة ووضع معايير تقييم الأدلة, تلك القواعد التي لا زالت مستخدمة حتى يومنا هذا. ولا زال هذا المجال بمبادئه وتطبيقاته يستخدم اليوم لفحص الوثائق التي تثار حولها تساؤلات, وبالتالي, لازالت مبادؤه وكثير من أدواته, مستخدمة أو لها استخدامات مشابهة في الإثبات الجنائي الرقمي[3].

وقد فرضت البيئة التكنولوجية تحديات كثيرة أمام بناء الثقة في الوثائق الرقمية نظراً لأن التكنولوجيا الحديثة أعادت المجتمع مرة أخرى إلى مبدأ الشك، وأصبحت الوثائق الرقمية مشكوك في صحتها، وبحاجة إلى من يبرهن على صحتها والحفاظ عليها صحيحة دائماً[4]. ولا شك أن التعرف على الوثائق من بين جميع الكيانات الرقمية التي تنتجها الأنظمة

---

[1] دينا محمود عبد اللطيف محمد. (2017). الإتجاهات الحديثة فى علم الوثائق (الدبلوماتيك) : دراسة تطبيقية على الوثائق العربية. "أطروحة دكتوراه"، جامعة الأزهر ، ص 78 – 79 .

[2] Montoya-Mogollón, J. B., & Troitiño Rodriguez, S. M. (2018). The Diplomatic and Digital Forensic Science in Born-Digital Records: The Quest for Authenticity. *Journal of Integrated OMICS*, *8*(1), p74-76.

[3] Cohen, F. B. (2015). Digital diplomatics and forensics: going forward on a global basis. *Records Management Journal*, *25*(1), p23 -24.

[4] Williams, C. (2005). Diplomatic attitudes: from Mabillon to metadata. *Journal of the Society of Archivists*, *26*(1), p2-3.

التفاعلية المعقدة, وتحديد صحتها, من أصعب القضايا التي تفرضها التكنولوجيا الرقمية على مجالات إنفاذ القانون, وإدارة الوثائق, ومهنة الأرشفة ومهنة القانون[5].

ومن أجل تمكين المتخصصين في دراسة الوثائق (الأدلة) لفهم الوثائق (الأدلة) الرقمية، استخدم مشروع إنتربارس المعرفة الدبلوماتية والأرشيفية التقليدية، وطبَّقها على جميع أنواع الكيانات الموجودة في مختلف البيئات الرقمية، وطور منها مجموعة جديدة من المعارف هدفت إلى تلبية الحاجات الحالية والمستقبلية. هذه المجموعة الجديدة من المعارف يمكن أن تسمى "دبلوماتيك الوثائق الرقمية"، وتعتبر نتاج علم الدبلوماتيك. وقد لا تكون كافية، ولكنها مخصصة للتعامل مع التحديات التي فرضتها البيئات الرقمية المعقدة، التي قد تتطلب أن تتم الإفادة من المفاهيم والمبادئ والأساليب المتقدمة في سياق التخصصات الأخرى للتأثير على الدبلوماتيك الرقمي، والعلم المنوط بذلك هو"علم الإثبات الجنائي الرقمي"(6). لكن، قبل التوسع في فكرة استخدامات جديدة لعلم قديم من الضروري أولاً أن نبدأ في توضيح مفهوم علم الدبلوماتيك الرقمي وعلم الإثبات الجنائي الرقمي ومن ثم شرح العلاقة بينهما.

أولاً- علم الوثائق (الدبلوماتيك) الرقمي وعلم الإثبات الجنائي الرقمي

1 - علم الوثائق (الدبلوماتيك) الرقمي Digital Diplomatics:

علم الدبلوماتيك الرقمي, هو تطور حديث لتخصص قديم, يدرس طبيعة الوثائق وأنواعها وخصائصها وبناءها ونشرها وتوابعها القانونية, يتناول المسألة الأولى, وهي التعرف على الوثائق الرقمية. بينما يتم تناول المسألة الثانية, وهي تقييم مدى صحة الوثائق الرقمية, حصرياً وبشكل غير مباشر, من قبل علم الإثبات الجنائي الرقمي[7]. ويجب الإشارة إلى أن ظهور الدبلوماتيك الرقمي كان نتاجاً للمرحلة الثالثة من مشروع InterPARES، وقد استخدمته كلاً من دورانتي و ماكنيل للتعبير عن العلم الذي يدرس الوثائق التي يُستخدم الحاسب الآلي لعرضها(8).

---

(5) Duranti, L., & Endicott-Popovsky, B. (2010). Digital Records Forensics: A New Science and Academic Program for Forensic Readiness. Journal of Digital Forensics, Security and Law,5(2), p45.

(6) Duranti, L. (2009). From digital diplomatics to digital records forensics. *Archivaria*, *68*, 39-66.

(7) Duranti, L., & Endicott-Popovsky, B. (2010). Digital Records Forensics, p45.

(8) دينا محمود عبد اللطيف محمد . (2017). الإتجاهات الحديثة فى علم الوثائق (الدبلوماتيك)، ص 231.

هذا التوجه إلى الدبلوماتيك الرقمي, والذي يعد نتيجة لمشروع InterPARES, يتيح لخبراء الأرشيف طريقة لتحليل هوية وتكامل الوثائق الرقمية في الأنظمة الإلكترونية وبالتالي تقييم مدى صحتها وتتبع نشأتها[9]. يتناسب الدبلوماتيك الرقمي جداً مع تحليل صحة الوثائق الرقمية وفقاً لتعريف علم الأرشيف للوثائق الرقمية[10], ولكنه يعتبر محدوداً عند اتساع موضوع التحليل ليشمل المواد الرقمية التي قد لا ينطبق عليها هذا التعريف الدقيق والضيق في نفس الوقت[11]. ويقوم الأرشيفيون حالياً بمشاركات بحثية مع ممارسي الإثبات الجنائي الرقمي والأدلة الجنائية الرقمية والحوسبة الجنائية من أجل تطوير وتوسيع نطاق الدبلوماتيك الرقمي في مجال الحفظ الرقمي، والتركيز على الصحة والمصداقية والدقة، بالنسبة إلى الأرشيف[12].

2 - علم الإثبات الجنائي

إنَ نظرية الإثبات هي الأساس الذي تقوم عليه قواعد الإجراءات الجنائية منذ لحظة وقوع الجريمة إلى حين صدور الحكم فيها من السلطة القضائية، بموجب السلطات الممنوحة لها. وقد طرأ على الإثبات الجنائي تطوراتٍ كبيرة بفضل الطفرة العلمية الهائلة في وسائل الإثبات، التي لم تكن معروفةً من قبل، فهي طفرة قامت على نظرياتٍ وأصول علمية دقيقة، واستطاعت أن تزود القاضي الجنائي بأدلة حاسمة تربط أو تنفي العلاقة بين المتهم والجريمة، وأصبح القضاء يُعول عليها كأدلة فنية ويؤسس عليها الأحكام بالإدانة أو البراءة[13].

---

(9) Duranti, L. (2005). The Long-term Preservation of Authentic Electronic Records: Findings of the InterPARES Project. Archilab, San Miniato, p 4.

(10) **يمكن تعريف الوثيقة وفقاً لعلم الأرشيف** بأنها مستند – أي معلومات مسجلة تم إنشاؤها أو تلقيها في سياق أحد الأنشطة العملية كمستند أو أداة أو كأحد منتجات هذا النشاط وتم الإحتفاظ بها لإجراء المزيد من العمليات عليها أو لغرض الرجوع إليها في المستقبل. انظر:

Duranti, L., & Rogers, C.(2012). Trust in digital records : An increasingly cloudy legal area . Computer law & Security review 28 , p524.

(11) Rogers, C. (2015). Diplomatics of born digital documents, p7.

(12) إسلام جمال صابر إبراهيم.(2021). الحوسبة السحابية للوثائق الإلكترونية، ص 75.

(13) محمد أحمد المنشاوي . (2012). سلطة القاضي الجنائي في تقدير الدليل الإلكتروني . مجلة الحقوق – الكويت،36 (2)، ص 516 – 517.

أ- مفهوم الإثبات الجنائي:

الإثبات في معناه القانوني: هو "إقامة الدليل لدى السلطات المختصة بالإجراءات الجنائية على حقيقة واقعة ذات أهمية قانونية، بالطرق التي يحددها القانون، لإثبات واقعة متنازع عليها"[14].

ويُقصد بالإثبات في المواد الجنائية بأنه: "الوسيلة التي يتم من خلالها إثبات وقوع الجريمة وعلاقة المتهم بها ونسبتها إليه".[15] فيراد به إثبات الوقائع لا بيان وجهة نظر المُشرع وحقيقة قصده، فالبحث في هذا يتعلق بتطبيق القانون وتفسيره وهو من عمل المحكمة[16].

كما يُعرَف الإثبات أيضاً بأنه " تأكيد حق متنازع فيه له أثر قانوني بالدليل الذي أباحه القانون لإثبات ذلك الحق"[17].

ب- علم الإثبات الجنائي الرقمي Digital Forensics Science

الإثبات الجنائي الرقمي هو فرع من علوم الإثبات الجنائي التي تهتم باستخدام المعلومات الرقمية التي يتم إنتاجها وتخزينها ونقلها بواسطة أجهزة الحاسب الآلي كمصدر للأدلة في التحقيقات والإجراءات القانونية[18].

وقد استخدم مصطلح الإثبات الجنائي الرقمي Digital Forensics في الأصل كمرادف لمصطلح الحوسبة الجنائية Computer Forensics ولكنه توسع ليشمل التحقيق في جميع الأجهزة الرقمية، مثل الهواتف المحمولة والكاميرات الرقمية والمدمجة وأجهزة الفاكس الرقمية الأخرى، بالإضافة إلى أجهزة الحاسب الآلي[19].

---

[14] عبد الرزاق السنهوري. (1968). الوسيط في شرح القانون المدني. ج 2. القاهرة : دار النهضة العربية، ص 13 – 14 .

[15] محمد ذكي أبو عامر .(2004). الإجراءات الجنائية . الإسكندرية : دار الجامعة الجديدة،227 .

[16] ممدوح عبد الحميد عبد المطلب.(2003). أنموذج مقترح لقواعد اعتماد الدليل الرقمي للإثبات في الجرائم عبر الكمبيوتر. دراسه مقدمه إلى مؤتمر الأعمال المصرفيه الإلكترونيه بين الشريعه والقانون, مجموعة أعمال المؤتمر , المجلد الخامس , الإمارات العربيه المتحده، ص2233 .

[17] جمال الخولي . (1994). إثبات الملكية في الوثائق العربية. ط1. القاهرة: الدار المصرية اللبنانية، ص18 .

[18] Pollitt, M. (2010, January). A history of digital forensics. In *IFIP International Conference on Digital Forensics* (pp. 3-15). Springer, Berlin, Heidelberg.

[19] طالب محمد جواد. (2012). الحاسب الجنائي: حاجة مُلحة في برامج دراسة القانون والحاسوب. مجلة كلية الرافدين الجامعة للعلوم، (30)، ص 2 - 3.

ويُقصد بالحوسبة الجنائية "جمع، وتحليل، والحفاظ على الأدلة المتصلة بالحاسبات لتقديمها إلى المحكمة"[20].

أما علم الإثبات الجنائي الرقمي فيعرف بعلم "تطبيق علوم الكمبيوتر وإجراءات الدراسة العلمية لغرض قانوني يشمل تحليل الشواهد الرقمية بعد تحليل مرجعية البحث المناسبة، وسلسلة الحفظ، والمصادقة باستخدام علم الرياضيات، واستخدام الأدوات المناسبة، والتكرار، والإبلاغ، وعرض الخبير الممكن."[21]

وبشكل **أكثر تحديداً**، قامت ورشة عمل أبحاث علم الإثبات الجنائي الرقمي، في عام 2001، **بتعريف" الإثبات الجنائي الرقمي"** باعتباره علم "استخدام المناهج العلمية في حفظ، وجمع، وتعريف وتحليل، وتفسير، وتوثيق، وتقديم الأدلة والشواهد الرقمية المستمدة من مصادر رقمية والتصديق عليها، وذلك بغرض تسهيل أو تعزيز إعادة تخيل طبيعة ما جرى من أحداث جنائية، أو المساعدة في توقع التصرفات غير المصرح بها التي تدمر العمليات المخططة."[22] **كما تم تعريفه** بأنه "تطبيق العلم والهندسة على المشكلات القانونية للأدلة الرقمية "[23].

3 - علاقة علم الوثائق (الدبلوماتيك) بعلم الإثبات الجنائي الرقمي

ارتبط علم الوثائق (الدبلوماتيك) منذ القدم بعلم القانون ولعل السبب في ذلك نشأته التي ارتبطت بإثبات صحة الوثائق والكشف عن المزيفات منها . وعلى الرغم من أن أهداف المتخصصين في الإثبات الجنائي الرقمي تختلف عن أهداف أمين حفظ الوثائق الموثوق به Trusted recordkeeper أو الوصي (المسئول عن العهدة) Custodian، في الوقت الحاضر،

---

[20] طالب محمد جواد. (2012). الحاسب الجنائي، ص 3.

[21] Zatyko, K .(2007). Commentary: Defining Digital Forensics. Forensic Magazine (Feb/March), p 1–5.

[22] Digital Forensics Research Workshop, 2001, p. 15, Retrieved from: http://www.dfrws.org/2001/dfrws-rmfinal.pdf (last visited 25 /5/ 2019).

[23] Pollitt, M.M. (2009). "Digital Forensics as a Surreal Narrative", in Peterson, G. and Shenoi, S. (Eds), *Advances in Digital Forensics*, Springer Berlin Heidelberg, Heidelberg, 306, p 3-15, Retrieved from: http://link.springer.com/10.1007/978-3-642-04155-6_1(last visited 1/1/ 2020).

إلا أنها تعتبر مماثلة لتلك الأهداف التي حملها الدبلوماتيك في القرن السابع عشر، وجعلت منه مقرراً دراسياً في كليات القانون الأوروبي في القرن الثامن عشر، وكان المشتغلون بعلم الوثائق (الدبلوماتيك) يومها هم بمثابة علماء الإثبات الجنائي، يستدعيهم القضاة لإقرار مدى صحة الوثائق في المحاكم عندما يُطعن في الحقوق التي تشهد عليها هذه الوثائق، ويطعن في جدارتها بالثقة[24]. وتعتبر ممارسات الدبلوماتيك ممارسات استقصائية بطبيعتها. وفي عملية النقد الدبلوماتي, يقوم خبراء الدبلوماتيك بتحليل الوثيقة للتحقق من العناصر التي توضح نشأة الوثيقة وعلاقاتها وموثوقيتها وصحتها وتحديد أماكنها في الوثيقة[25]. ومن هنا تظهر أهمية علم الوثائق (الدبلوماتيك) بالنسبة لعلم الإثبات الجنائي الرقمي، ودوره في إثبات صحة الوثيقة الرقمية أو الدليل الرقمي، حيث ارتبطت نشأة علم الوثائق (الدبلوماتيك) الرقمي أيضاً بعلم الإثبات الجنائي الرقمي أو التحقيق الجنائي الرقمي Digital Forensics، وقد كتب الدبلوماتيون المعاصرون عن استخدام علم الوثائق (الدبلوماتيك) في الإثبات الرقمي، وكذلك فعل رجال الأدلة الجنائية الرقمية، حيث يُمكن الجمع بين مبادئ علم الدبلوماتيك الرقمي وعلم الإثبات الجنائي الرقمي[26]. وقد سعى كلاهما للحصول على الدعم الفكري للتخصصات التي تدرس نفس النوع من المواد التي هي موضوع تحليلهم: الوثائق في حالة علم الدبلوماتيك، الكيانات المختلفة والمواد، والآثار في حالة علم الإثبات الجنائي. وهكذا، وفي حين دمج علم الوثائق نظريته مع نظرية علم الأرشيف لضمان نشأة وثائق جديرة بالثقة تستخدم بعد ذلك كمصادر يستخلص منها الحقائق التاريخية والقانونية وغيرها، فقد اعتمد علم الإثبات الجنائي الرقمي على دعم التخصصات التي درست المواد قيد التحقيق بشكلٍ أفضل، مثل الطب والرياضيات والهندسة وعلوم الحاسبات.

وكان فريدرك كوهين[27] عالم الإثبات الجنائي الرقمي أول من أدخل مجال الدبلوماتيك في أدبيات الإثبات الجنائي الرقمي، وهو الآن أيضاً باحث في مشروع InterPARES

---

[24] Duranti, L. (2009). From digital diplomatics to digital records forensics. *Archivaria, 68*, p43 .

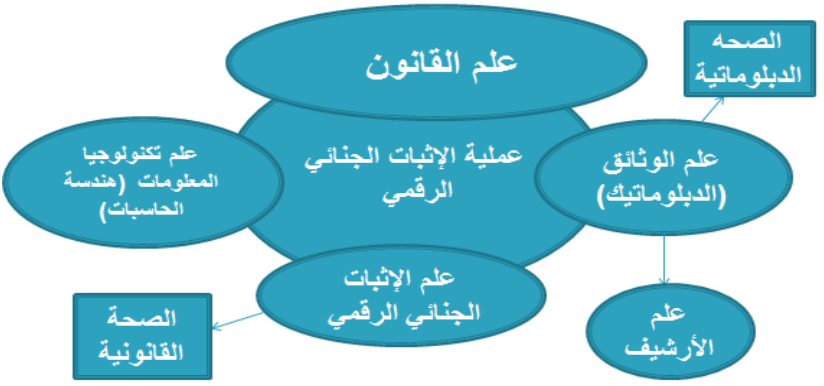
[25] Rogers, C. (2015). Diplomatics of born digital documents, p8.

[26] دينا محمود عبد اللطيف محمد . الإتجاهات الحديثة فى علم الوثائق (الدبلوماتيك)،ص 75 – 76.

[27] فردريك كوهين هوعالم الإثبات الجنائي الرقمي حصل على درجة الماجستير في علوم المعلومات، كما حصل على درجة الدكتوراه في الهندسة الكهربائية، والدكتوراه الفخرية في علوم الحاسب الآلي. واشتهر بأنه

Trust في جامعة كولومبيا البريطانية UBC[28]. ويجب الإشارة إلى أن الوثائقيين في الدول الأوروبية وشمال أمريكا يعملون بالفعل في مكاتب التحقيق الجنائي الرقمي.

يتضح مما سبق، أن عملية الإثبات الجنائي للوثائق الرقمية تتطلب تحقيق التكامل بين عدة علوم، وهذه العلوم هي، علم الوثائق (الدبلوماتيك)، الذي يحقق الصحة الدبلوماتية، وعلم الإثبات الجنائي الرقمي الذي يحقق الصحة القانونية ويُساعد في ذلك علم الأرشيف وعلم تكنولوجيا الحاسبات وكل هذه العلوم تعمل في إطار علم القانون. مما يوضح تكامل هذه العلوم مع علم الإثبات الجنائي الرقمي كما هو موضح في الشكل رقم (1).



شكل رقم (1) يوضح التكامل بين علم الدبلوماتيك وعلم الأرشيف وعلم تكنولوجيا الحاسبات وقانون الأدلة والإثبات الجنائي الرقمي

ثانياً - مناهج الدبلوماتيك الرقمي والإثبات الجنائي الرقمي:

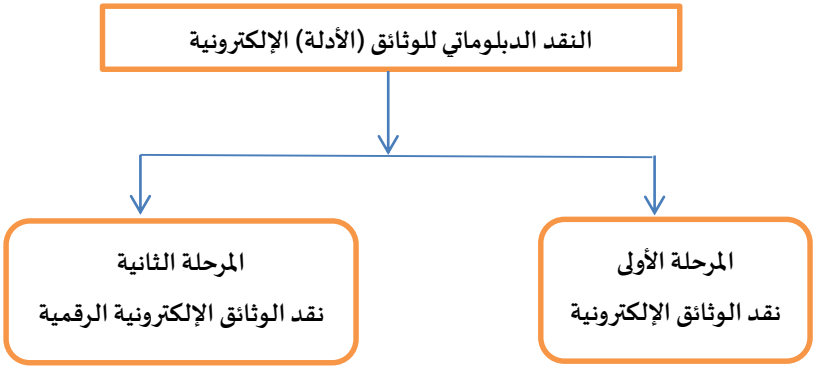
1 – منهج الدبلوماتيك الرقمي

قدَم مشروع انترباررس InterPARES في المرحلة الأولى عام 2000 نموذجاً للنقد الدبلوماتي للوثائق الإلكترونية بصفة عامة، ولم يواجه تطبيقه على قواعد البيانات وأنظمة

الشخص الذي عرَف مصطلح "فيروس الحاسب" ومخترع معظم تقنيات الوقاية من فيروسات الحاسب المستخدمة على نطاق واسع. ويُعتبر باحث مبتكر في استخدام الخداع لحماية المعلومات، ورائد في النهوض بعلم الإثبات الجنائي الرقمي. انظر:.. Cohen, F. B. (2015). Digital diplomatics and forensics, p44

[28] Rogers, C. (2015). Diplomatics of born digital documents, p10.

إدارة الوثائق صـعوبات كبيرة، ولكن ثبت أن اسـتخدامه في المرحلة الثانية من InterPARES، التي ركزت على الأنظمة التفاعلية والديناميكية، كان مسـتحيلاً. لذلك قدم في المرحلة الثانية طريقة أخرى للنقد الدبلوماتي تعتمد على كيفية التأكد من كون الكيان الرقمي وثيقة أم لا. وبناءً على ما سبق، فإن عناصر النقد في المرحلة الأولى تختص بالوثائق الإلكترونية الثابتة مثل البريد الإلكتروني والفيديو والميكروفيلم، أما نقد الوثائق الإلكترونية الرقمية التفاعلية والديناميكية ووثائق الخط المباشر فهو النقد المطروح في المرحلة الثانية والثالثة من المشروع كما هو موضح في الشكل رقم (2)، وهكذا تم إنشاء نموذج جديد يعمل مع الأنظمة شديدة التعقيد التي تم فحصها في سياق دراسات الحالة المختلفة للمشروع[29].



شكل رقم (2) يوضح مراحل مشروع انترباس للنقد الدبلوماتي للوثائق الإلكترونية

النقد الدبلوماتي للكيانات الرقمية :

يبدأ النقد الدبلوماتي للكيانات الرقمية كما هو موضح بالشكل رقم (3):

- بتقديم وصف للبيئة التكنولوجية التي توجد فيها الكيانات، ووصف العروض الرقمية والوثائقية، ثم التحقق من وجود أو عدم وجود المكونات الستة للوثيقة، مع إيلاء اهتمام خاص لأخر متطلبين، وهما الشكل الثابت والمحتوى المستقر.

---

[29] دينا محمود عبد اللطيف محمد . الإتجاهات الحديثة في علم الوثائق (الدبلوماتيك)، ص 355. انظر أيضاً:
Appendix 1. Template for Analysis," in Duranti, L. (2001). The long-term preservation of authentic electronic records. See also "Appendix 7. Diplomatic Analysis Template," in Duranti and Preston.

- فحص الإجراء الذي شارك فيه الكيان الرقمي.
- فحص العلاقات الفكرية بين الكيانات، والعلاقة بين كل كيان وكل شخص له دور في إنشائها.
- وأخيرا، يتم تحليل السياقات المختلفة تحليلا عميقا، وخاصة السياق الإجرائي إذا تم ربط الكيان بإجراء بعينه، والسياق الوثائقي إذا تم ربط الكيان صراحة بالكيانات الأخرى داخل النظام أو خارجه الذي وصفها بأنها وثائق، والسياق التكنولوجي إذا كان لدى الكيان صلات مباشرة مع الكيانات الرقمية الأخرى.

ويجب أن يستنتج النقد الدبلوماتي ما إذا الكيان الرقمي هو وثيقة أم لا. **وإذا كان الجواب بلا**، ينبغي أن يبين التحليل ويوضح أكثر وضع الكيان الرقمي كمجموعة من البيانات، أو كمنشور أو وثيقة محتملة، كما يجب أن يوضح الخصائص المحددة، والسمات والتصرفات، والتوصية بالإجراءات الأكثر ملائمة تبعا لغرض البحث.

وإذا **كان الجواب بنعم**، يتم إجراء تحليل أكثر تفصيلا لتحديد ما إذا كانت الوثيقة جديرة بالثقة، وما هي الخصائص البارزة التي هي في حاجة إلى الحماية من أجل الحفاظ على هوية الوثيقة وتكاملها بمرور الوقت، وما العناصر الشكلية التي تعبر عن هذه الخصائص المميزة للوثيقة، وما المكونات الرقمية التي توجد فيها الوثائق[30].

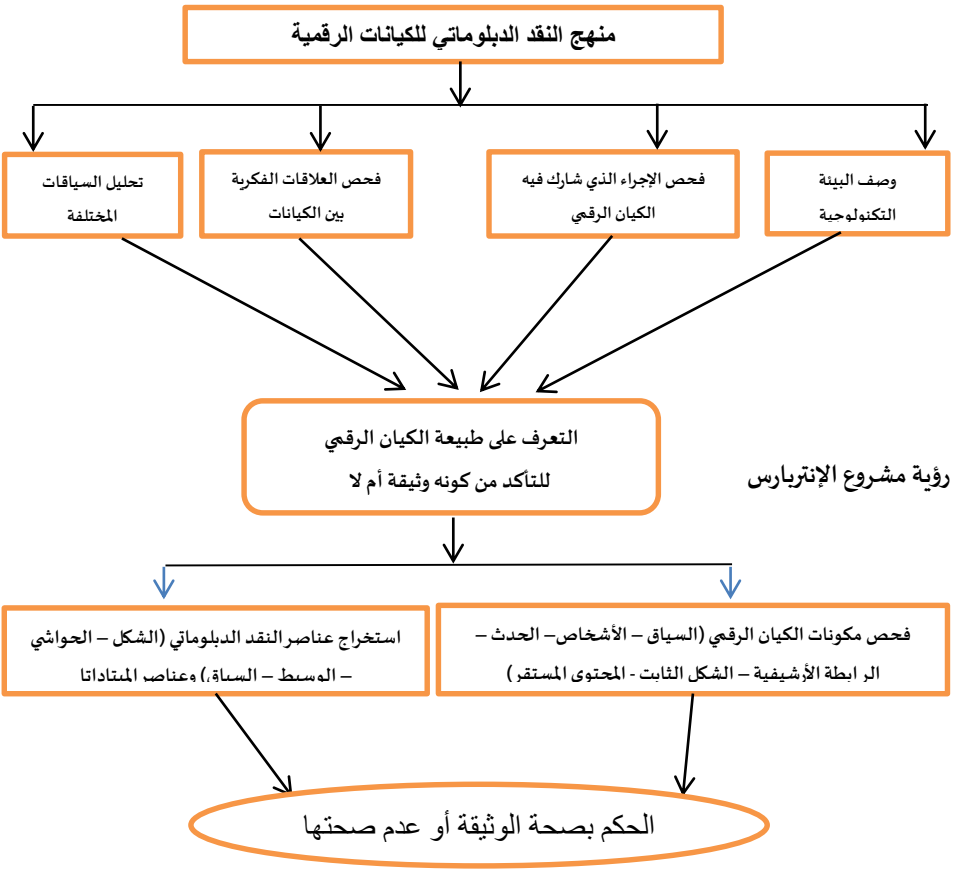
وبناءً على ما سبق، فقد رأى العاملون في مشروع الإنتربارس ضرورة أن يبدأ الدبلوماتي أولاً بفحص مكونات الكيان الرقمي والتعرف على طبيعته للتأكد من كونه وثيقة أم لا ومن ثم استخراج عناصر النقد الدبلوماتي منها كما هو موضح في الشكل رقم (3)، ولذلك أصبح النقد يتكون من :

- فحص مكونات الكيان الرقمي (السياق – الأشخاص المشاركين في انشائه – حدث يكون للوثيقة دور فيه أو موضوع الوثيقة – الرابطة الأرشيفية – الشكل الثابت - المحتوى المستقر) للتحقق من وجود أو عدم وجود المكونات الستة لوجود الوثيقة، مع إيلاء اهتمام خاص لأخر متطلبين، الشكل الثابت والمحتوى المستقر.
- التعرف على خصائص الوثيقة الدبلوماتية الإلكترونية، وذلك من خلال استخراج عناصر النقد الدبلوماتي (الشكل – الحواشي – الوسيط – السياق)، وعناصر الميتاداتا، وذلك في حالة التأكد من وجود مكونات الوثيقة الستة .

---

[30] Duranti, L. (2009). From digital diplomatics, p62.

- الحكم بصحة الوثيقة أو عدم صحتها[31].



شكل رقم (3) يوضح منهج النقد الدبلوماتي للكيانات الرقمية

2 - منهج الإثبات الجنائي الرقمي

يتمثل المنهج الرئيس للإثبات الجنائي الرقمي في الحصول على الوثائق (الأدلة) الرقمية والممارسات المتصلة بها وتحليلها وتقييمها مع ضمان الحفاظ على سلامتها[32]. وتُعد عملية

---

[31] دينا محمود عبد اللطيف محمد . نفس المرجع، ص 355.

[32] Agarwal, A., Gupta, M., Gupta, S., & Gupta, S. C. (2011). Systematic digital forensic investigation model, p 119.

الحصـول على الوثائق (الأدلة الجنائية الرقمية) أمر صـعب الوصـول إليه لما تتطلبه من خبرة ومهـارة كبيرة في مجـال الحـاســب الآلي[33]، ويرجع ذلـك إلى تعـدد صــور وأشــكـال الجرائم المعلوماتية، ما بين مهاجمة المعلومات بغرض تدميرها أو الإسـتيلاء عليها أو قد يكون المقصـود بالهجوم هو الأجهزة كنشــر فيروس يعمل على إتلاف وحداته الرئيســة مثلاً، أو قد يكون الأمر مجرد اختراق لكلمة سر خاصة ببنك أو مؤسسة كبرى بغرض الإحتيال والحصول على الأموال، ولما كانت عملية تجميع الأدلة العلمية الجنائية في الجرائم المعلوماتية، من أهم وأصـعب الأمور التي تواجه عملية الإثبات الجنائي، لذلك كان لزاماً أن يتم اللجوء إلى خبير قضــائي معلوماتي (متخصص)، لاشتقاق الدليل العلمي الفني الجنائي.

الخبير المعلوماتي هو الخبير المتخصــص والمدرب على معـالجـة جميع أنواع الأدلـة الرقمية وفحصـها وتحليلها[34]، يسـتطيع خبراء الإثبات الجنائي للوثائق (الأدلة) الرقمية القيام بدور الشـاهد الخبير بسـبب مسـؤوليتهم عن العملية الاسـتقصـائية. ولكنهم يختلفون عن خبراء الأرشــيف بالتزامهم بمجموعة مختلفة من المتطلبات, وهي الشــهادة العلمية التي تُعطى لتبرير استخدام أدواتهم وأساليبهم في التحقق من الدليل الرقمي والتأكد من صحته. وقد تخضع هذه الشـهادة العلمية لاختبار المصـداقية في جلسـة دوبيرت Daubert.[35] لذلك يجب على الخبير أن يكون على المام تام ببعض العلوم، ومنها علم الحاســبات وعلم الأدلة الجنائية وعلم التحليل السـلوكي للأدلة الرقمية، وعلم الوثائق (الدبلوماتيك) الرقمي وعلم الأرشــيف، حيث أن علوم الحاســبات تقـدم المعلومـات التكنولوجيـة الـدقيقـة وهي مطلوبـة لفهم المظهر أو الهيئـة أو الكينونة الفريدة للدليل الرقمي بينما علوم الأدلة الجنائية الرقمية من شـأنها أن تقدم منظوراً علمياً لتحليل أي شـكل من أشـكال الأدلة الرقمية أي أنها تهتم بمعالجة المشـاكل الأسـاسـية المسـتمدة من طبيعة التكنولوجيا الرقمية والمتمثلة في مشـكلتي التعقيد والكم. وتسـاهم علوم

---

[33] محمد عبيد سيف سعيد المسماري.(2007). الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية: دراسة تطبيقية مقارنة . بحث مقدم في المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، الرياض : جامعة نايف العربية للعلوم الأمنية، ص34.

[34] محمد الأمين البشري .(2004). التحقيق في الجرائم المستحدثة . بحث مقدم إلى المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، ط 1، جامعة نايف العربية للعلوم الأمنية – الرياض، ص243 .

[35] Rogers, C.(2013). Digital Records Forensics, p 9.

التحليل السلوكي للأدلة الرقمية في الربط المحدد بين المعارف التكنولوجية وبين الطرق العلمية لإستخلاص الدليل الرقمي، لفهم أفضل للسلوك الإجرامي التقني[36]. أما علم الدبلوماتيك الرقمي الأرشيفي فهو يُساعد على فهم نشأة الوثائق الرقمية (سياق وأشخاص وإجراءات وتصرفات)، كما يُعطي المفاهيم والأدوات للأرشيفي عن طبيعة الوثائق، وكيفية معاملة الوثائق في النظم الإلكترونية[37]. لذلك فإنَ الفهم العميق للوثائق الرقمية المكتسب من خلال تحليل علم الدبلوماتيك الرقمي سيكون بلا شك مفيدا لخبراء الإثبات الجنائي الرقمي، الذين تتمثل مهمتهم الأساسية وذات الحساسية الشديدة في الحصول على أدلة من البيئة الرقمية دون التدخل فيها، أي الحفاظ على هوية سليمة للأدلة وحماية سلامتها، وكذلك سلامة النُسخ التي يقدمونها[38].

نموذج الإثبات الجنائي للوثائق الرقمية (Digital Records Forensics (DRF:

هو نموذج تم تصميمه بغرض دراسة نقاط الإلتقاء بين أهداف ووظائف علم الأرشيف وعلم الإثبات الجنائي للوثائق الرقمية (نموذج DRF). تكمن قيمة النموذج المقترح لمشروع الإثبات الجنائي للوثائق الرقمية DRF, في مشاركة المعرفة بين التخصصات العلمية (الإثبات الجنائي الرقمي والدبلوماتيك الرقمي وعلم الأرشيف، وقانون الأدلة) [39]. كما يسمح هذا النموذج بتطوير البرامج التعليمية التي تخرج المتخصصين الذين يملكون القدرة على الحصول على الوثائق الدقيقة والصحيحة التي يمكن الإعتماد عليها وكذلك إنشائها وتقييمها وضبطها وحفظها طوال فترة الإحتياج إليها[40].

يهدف نموذج الإثبات الجنائي للوثائق الرقمية DRF إلى توحيد مفاهيم ممارسة الإثبات الجنائي الرقمي، ووضع حجر الأساس لتكامل هذا العمل مع نموذج سلسلة حفظ إنترباس Chain of Preservation (CoP) لإدارة الوثائق على مدار دورة حياتها[41].

---

[36] خالد ممدوح إبراهيم . (2009). فن التحقيق الجنائي في الجرائم الإلكترونية. ط1. الأسكندرية: دار الفكر الجامعي، ص 118.

[37] دينا محمود عبد اللطيف محمد . نفس المرجع، ص 264 .

[38] Duranti, L. (2009). From digital diplomatics, p62.

[39] Rogers, C.(2013). Digital Records Forensics, p5.

[40] Duranti, L., & Endicott-Popovsky, B. (2010). Digital Records Forensics, p46-47.

[41] Duranti, L., & Preston, R. (2008). Research on Permanent Authentic Records, p15.

قـام الفريق البحثي الخـاص بـالفحص الجنـائي للوثـائق الرقميـة بعمـل نموذج لعمليـة إجراء تحقيق جنائي رقمي، بغرض تقييم اللحظات التي يمكن فيها التحقق من الوثائق وتقييم مدى صـحتها وإدارة وحفظ موثوقيتها وسـلامتها, وفقا لمفهوم علم الدبلوماتيك الأرشـيفي وقوانين الأدلة. كان الهدف من هذا النموذج هو تكامل الشرط الجوهري للإثبات الجنائي للأدلة الرقمية المتمثل في تثبيت وتوثيق وحماية تسـلسـل الأوصـياء, مع نموذج سـلسـلة حفظ إنتربارس CoP لحفظ الوثائق الرقميـة التي يمكن افتراض صـحتها وموثوقيتها. وكان الهـدف من الأنشـطة المقـدمـة في هـذا النموذج هو التـأكـد من نشـأة أو جمع الوثـائق الرقميـة الجـديرة بـالثقـة لاستخدامها كأدلة, والتأكد من صيانتها طوال فترة عملية التحقيق القضائي وحفظها على المدى البعيد لأغراض المسؤولية أو الرجوع إليها أو إجراء مزيد من العمليات عليها.

تولى الفريق مهمة عمل نموذج لعملية الفحص الجنائي الرقمي من وجهة نظر قوات إنفاذ القانون. وبالتالي فالنتيجة هي التحقق من وإنتاج مواد رقمية صـالحة للإثبات يمكن أن تقبلها المحكمة كدليل. ولكن النموذج كان يهدف للاتسـاع بشـكل كاف لينطبق على تحليل الاستجابات الأمنية.

وقد تضـمن النموذج جميع مراحل دورة حياة المواد الرقمية التي قد تخضـع للفحص الجنائي في تحقيقات الجرائم أو الأحداث الأمنية. يضـع النموذج هذه المواد في سـياق المنظومة القضـائية ويعتبر عملية التحقيق بمجملها كميزان A balance بين المدخلات المتاحة, وعقبات التحقيق أو ضـوابطـه, والآليـات المسـتخـدمـة في التحقيق, والنتـائج المرجوة أو مخرجـات التحقيق[42].

قيود وضو ابط التحقيق الجنائي الرقمي :

يجرى الفحص الجنائي الرقمي دائما في ظل قيود وضـوابط يفرضـها النظام القضـائي الذي يجري التحقيق في إطاره, وفي ظل الموارد المتاحة لإجراء التحقيق, وفي ظل مبادئ الإثبات الجنائي الرقمي المعروفة في إطار التطور المنهجي والنظري لهذا المجال العلمي.

وتشـمـل الموارد المتـاحـة للمحقق الموظفين والـدعم المـالي والأدوات والتكنولوجيـا والمعرفة المتخصـصـة أو المعرفة بالمجال. وقد تطورت مبادئ الفحص الجنائي الرقمي لتدعم أغراض تحقيقات الإثبات الجنائي الرقمي، وقام عدد من الخبراء في هذا المجال بتلخيصـها, وفي

[42] Rogers, C.(2013). Digital Records Forensics, p 9.

ظل المبدأ الإســترشــادي الذي يقول: "إن الإجراء المتخذ لتأمين الأدلة الإلكترونية وجمعها لا يجب أن يحدث أي تغيير في هذه الأدلة"[43], تشمل هذه المبادئ المفاهيم التالية:

- السلامة
- الصحة
- قابلية إعادة الإنتاج
- عدم التداخل
- البساطة

وهذه المبادئ نفســها تخضــع لتنظيم قوانين الأدلة, والمعايير الوطنية والدولية ذات الصــلة، ثم أخيرا, يواجه التحقيق أيضــا عقبة الهيكل الوظيفي الذي يجري في ظله التحقيق بشكل مباشر.

الآليات الضرورية لإجراء عملية الفحص الجنائي للوثائق الرقمية:

يحتاج الأمر للكثير من العناصــر من أجل إجراء تحقيق جنائي رقمي ناجح للوثائق (الأدلة) الرقمية. وفي الغالب تشمل هذه العناصر الدعوى القضائية والمحققين وخبراء الأدلة الجنائية والأدوات والأجهزة التي يستخدمونها. ويوضح النموذج أن مديري الوثائق أيضا يلعبون دوراً مهما في عملية الفحص الجنائي للوثائق الرقمية، وذلك بتحققهم من الوثائق وتقديم خبرتهم العملية المتخصصة في المسائل التي تتعلق بالوثائق، مثل قضايا الخصوصية وتقييم صحة الوثائق والموثوقية والدقة واشتراطات حفظ الوثائق والوصول إليها.

مدخلات عملية الفحص الجنائي للوثائق الرقمية:

في الحقيقة, تتمثل المدخلات في عملية الفحص الجنائي في المعلومات أو العناصر التي تنشــأ خارج النشــاط المصــمم له النموذج. عند القيام بتحقيق الأدلة الجنائية الرقمية لإحدى الجرائم أو انتهاك النظام, لا بد من وجود مؤشــر, مثل بعض المعلومات عن نشــاط غريب أو مريب أو إجرامي. قد ينتج عن هذا المؤشر شكوى, سواء مكتوبة أو شفوية للتحقيق فيها. وقد يتم إجراء النشــاط في منظومة رقمية حية, أو في مواد رقمية يجمعها المحقق, أو مواد ينتجها

(43) US Department of Justice. (2001). *Electronic Crime Scene Investigation: A Guide for First Responders*. Washington, DC. Retrieved from: http//:www.ojp.usdoj.gov/nij (last visited 14/12/2020).

طرف آخر. وقد يتم تدعيم النشاط أيضا بالوثائق التي انشأها المحقق, أو بالأدلة التي تفرج عنها المحكمة مصحوبة بالوثائق. ومن هذا المنطلق فإن المدخلات تشمل كل تصريحات تحريز وتفتيش المواد والوسائط الرقمية والمعلومات المتعلقة بالواقعة قيد التحقيق والمواد والأنظمة والوسائط الحية والساكنة المطلوب فحصها.

مخرجات عملية الفحص الجنائي للوثائق الرقمية:

هناك الكثير من المخرجات التي يمكن تصنيفها جميعا على أنها أدلة تقدم للمحكمة أو المجلس, ومواد مخزنة أو محفوظة من القضية وتحقيقاتها, وممتلكات عينية يمكن إعادتها إلى صاحب الحق فيها عند انتهاء التحقيق أو المحاكمة. وبناءً عليه فإن المخرجات تشمل الوسائط الرقمية المصادرة قانوناً, والوثائق التفصيلية لكل الإجراءات التي تم اتخاذها, وصور الفحص الجنائي للوسائط المطلوب حفظها وفحصها[44].

إجراءات الفحص الجنائي الرقمي

يبرز النموذج ستة أنشطة رئيسة في الفحص الجنائي للوثائق الرقمية هي:

(1) الإعداد للفحص الجنائي

(2) جمع المواد الرقمية الصحيحة

(3) فحص المواد الرقمية

(4) الوصول للنتائج

(5) تقديم حزمة الأدلة

(6) إدارة مواد القضية.

(1) **الإعداد لعملية التحقيق الجنائي:**

يبدأ الإعداد لعملية التحقيق بوجود مؤشر معين وهو جريمة أو أمر قانوني آخر أو مسألة أمنية تقود إلى تحقيق وبحث عن أدلة محتملة أنشأتها الأجهزة التكنولوجية (مثل الحاسب الآلي أو الأجهزة المحمولة أو أجهزة شبكية إلخ). وبمجرد ابتداء المؤشر للتحقيق, يبدأ الإعداد بجمع المعلومات المساعدة والوثائق والأدوات وخطة الفحص الجنائي[45]. وقد يشمل

---

[44] Rogers, C.(2013). Digital Records Forensics, p 14 - 16.

[45] Venter, H. S., & Kigwana, I. (2018). A digital forensic readiness architecture for online examinations. *South African Computer Journal*, *30*(1), 1-39.

المحققون قوات إنفاذ القانون أو خبراء قانون وخبراء في تكنولوجيا المعلومات والشبكات ومتخصصين في الإثبات الجنائي للأدلة الرقمية[46].

(2) **جمع الوثائق (الأدلة) الرقمية الصحيحة:**

إنَ عمليات ضبط وحجز وتأمين وفحص الوثائق (الأدلة) الجنائية الرقمية المخزنة في شبكات المعلومات، هي التحدي الذي يواجه أجهزة العدالة الجنائية في ظل التقدم التكنولوجي، ويتطلب مواجهة هذا التحدي الجديد بناء قدر من التعاون والثقة بين أجهزة تنفيذ القانون والمؤسسات التي تقوم بتقديم خدمات المعلومات والإتصالات، لذلك يجب إعداد خبراء يجمعون بين المعرفة القانونية ومهارة التحقيق وعلوم تقنية المعلومات، وبالتالي فإن الشخص الذي يُكلف بجمع الوثائق (الأدلة) الرقمية وفحصها وتحليلها هو الخبير المتخصص والمُدرب على معالجة جميع أنواع الوثائق الرقمية وفحصها وتحليلها كما ذكرنا سابقاً[47].

وبمجرد اتخاذ قرار إجراء التحقيق الجنائي الرقمي بناء على أحد البلاغات, يقوم المحققون بجمع المواد الرقمية الصحيحة التي قد تكون ذات صلة بالتحقيق. يتمثل نشاط جمع المواد الرقمية الصحيحة بكل الأنشطة التي يجريها محقق الأدلة الجنائية الرقمية لتأمين مسرح الجريمة أو موقع الحدث, والاستحواذ على المواد المراد فحصها وحفظ مسرح الجريمة مقدما من خلال التصوير الجنائي لهذا المسرح[48]. وقد يشمل هذا الإجراء أحد أو كل الأنشطة التالية:

- تأمين وتوثيق مسرح الجريمة.
- تقييم النظام أو الأنظمة الرقمية التي سيجري فحصها.
- نسخ أو طباعة محتويات الملفات من الخادم، أو تسجيل حركة مرور الشبكة، وما إلى ذلك[49]
- مصادرة الوسيط الرقمي الذي يُعتقد احتواؤه على أدلة مهمة وذات صلة بالتحقيق والاحتفاظ به في مكان آمن.

---

(46) Rogers, C.(2013). Digital Records Forensics, p 15-16.

(47) Rosenblatt, K. S. (1995). *High-technology crime: investigating cases involving computers*. San Jose, CA: KSK Publications, p21.

(48) Agarwal, A., Gupta, M., Gupta, S., & Gupta, S. C. (2011). Systematic digital forensic investigation model. *International Journal of Computer Science and Security (IJCSS), 5*(1), 118-131.

(49) Ganesh, V. (2015). Digital Forensics. *International Journal* of advanced research, *3*(11), p909.

- التقاط صور جنائية لوسيط التخزين.
- توثيق جميع المواد التي تم جمعها[50].

ويجب الإشـــارة إلى، أن الوثائق (الأدلة) الجنائية الرقمية مثل غيرها من الأدلة المادية تحتاج إلى التوثيق والتأمين بالقدر الذي يكفل لها المصداقية، وذلك لعدة أسباب منها:

- عملية التوثيق تضمن الحفاظ على الشكل الأصلي للوثائق (الأدلة) الرقمية، وبالتالي تؤكد على مصـــداقية الدليل وعدم تعرضـــه لتحريف أو تعديل. على ســـبيل المثال، الصـــورة المسجلة بالفيديو يمكن الإستعانة بها في تأكيد مدى صحة الحوار بين طرفين عن طريق مطابقة النص الرقمي مع النص المصور على الشاشة.
- التوثيق يمكن المحققين الذين يقومون بجمع الأدلة من الإدلاء بشـــهاداتهم أمام القضـــاء حول مطابقة الوثائق (الأدلة) التي قاموا بجمعها مع تلك المقدمة أمام المحكمة. ويعتبر فشل المحقق في التمييز بين أصل الدليل وصورته أمام القضاء سبباً في بطلان الدليل(51)، وهنا يجب التأكيد على دور علم الدبلوماتيك، حيث أنَ الوظيفة الأولى للنقد الدبلوماتي هي تمييز أصل الوثيقة عن نسختها بغرض تحديد درجة صحة ومصداقية الوثيقة التي يتم فحصها(52).
- من المهم توثيق مكان ضبط الدليل الرقمي في حالة إعادة تكوين الجريمة، لأن تشابه أجهزة الحاسب وملحقاتها يجعل من الصعب إعادة ترتيبها دون وجود توثيق سليم ومفصل يحدد الأجزاء والملحقات وأوضاعها الأصلية بدقة.
- يُشـــكل التوثيق جزءاً من عمليات حفظ الأدلة الرقمية حتى انتهاء إجراءات التحقيق والمحاكمة، إذ أن التوثيق يشـــمل تحديداً دقيقاً للجهات التي تحتفظ بالأدلة وقنوات تداولها والتي ينبغي حصرها في نطاق محدود قدر الإمكان[53].

---

(50) Duranti, L. (2009). From digital diplomatics, p63.

(51) Saferstein, R. (1998). *Criminalistics*: An Introduction to Forensic Science, Upper Saddle River, NJ: Prentice Hall, p 34.

(52) سلوى علي ميلاد. (2018) . علم الوثائق (الدبلوماتيك) الحديث، ص 23.

(53) Saferstein, R. (1998). Op.cit, p 34.

عند توثيق الدليل الرقمي يجب التأكد من أين وكيف ومتى وبواسطة من تم ضبط الدليل وتأمينه. كما أنه من الضروري توثيق الأدلة الرقمية بعدة طرق كالتصوير الفوتوغرافي، والتصوير بالفيديو، وطباعة نسخ من الملفات المخزنة في جهاز الحاسب أو المحفوظة في الأقراص[54]. وعند حفظ الأدلة الرقمية على الأقراص والشرائط يجب تدوين البيانات التالية على كل منها:

- التاريخ والوقت.
- توقيع الشخص الذي قام بإعداد النسخة.
- إسم أو نوع نظام التشغيل.
- إسم البرنامج أو الأوامر المستعملة لإعداد النُسخ.
- المعلومات المضمنة في الملف المحفوظ[55].

كما تستخدم خوارزمية التوقيع الرقمي لمضاهاة الأدلة الرقمية الأصلية مع النسخ، للتأكد من صحتها وعدم تعرضها لأي تلاعب أو تغيير.

ويرى بعض الخبراء أن عملية جمع الأدلة الرقمية في الجرائم المعلوماتية التي تتم عبر الشبكة العالمية (الإنترنت)، تتم عبر ثلاث مراحل:

المرحلة الأولى: تجميع المعلومات المخزنة لدى الطرف الثالث مقدم الخدمة Third – party servers، من خلال تتبع الحاسبات الخادمة التي دخل فيها المجرم المعلوماتي ويحاول إيجاد أي أثر له[56].

المرحلة الثانية: مرحلة المراقبة، حيث يتم مراقبة هذه الحاسبات بطرق مختلفة، نذكر منها ما يلي:

- استخدام برامج مراقبة يمكن تحميلها للبحث عن المعلومات المشتبه بها وتسجيل بيانات الدخول والخروج بالموقع(57).

---

(54) Duranti, L. (2009). From digital diplomatics, p63.

(55) محمد الأمين البشري.(2008). تأهيل المُحققين في جرائم الحاسب الآلي وشبكات الإنترنت. المجلة العربية للدراسات الأمنية والتدريب. جامعة نايف العربية للعلوم الأمنية – الرياض، ص30.

(56) خالد ممدوح إبراهيم . (2009). فن التحقيق الجنائي في الجرائم الإلكترونية، ص300.

(57) ابتسام بغو. (2016). إجراءات المتابعة الجزائية في الجريمة المعلوماتية. "أطروحة ماجستير"، جامعة العربي بن مهيدي أم البواقي، ص 25.

- استخدام نوع من الحشرات أو Bugs، وهي أجزاء توضع في الحاسب الآلي لمراقبته.
- استخدام كاميرات مراقبة لشاشة الحاسب الآلي معدة للإستخدام التجاري، وأبسط الطرق لمراقبة الحاسب الآلي هي الدخول لمكان وجوده وزرعه.
- استخدام وسيلة أخرى أصعب قليلاً، وهي زرع فيروس حاسب أو دودة من نوع حصان طروادة، هذه الوسيلة تستطيع مراقبة أكثر من جهاز واحد ولكن يجب عدم السماح للفيروس بالإنتشار، وإلا سوف يصبح هدفاً لبرامج الدفاع ضد الفيروسات.

المرحلة الثالثة: ضبط الأجهزة المشتبه بها وفحصها فحصاً فنياً

يبدأ في هذه المرحلة عمل الخبير المعلوماتي في فحص النظام المشتبه به بمكوناته المادية ومكوناته البرامجية، سعياً لاشتقاق الدليل المادي لتقديمه لجهة التحقيق أو الحكم، لتقرير مدى وقوع الجريمة باستخدام النظام المضبوط من عدمه، ولتقرير إدانة المتهم أو تأكيد براءته، وذلك جميعه وفق القواعد الفنية المتعارف عليها والمتبعة في مجال الخبرة المعلوماتية، مع مراعاة القواعد القانونية لمبدأ المشروعية[58].

(3) فحص المواد الرقمية:

يشمل هذا النشاط إعداد المواد التي تم جمعها للفحص, واستخلاص وفحص الأدلة الرقمية المحتملة, وإعادة التركيب الافتراضي للأحداث, وتوثيق كل الإجراءات[59].

ونظراً لأن مهمة الخبير تقتصر على التحقيق في الدعوى وإبداء رأيه في المسائل الفنية التي يصعب على القاضي استنتاجها دون المسائل القانونية[60]، لذلك يجب أن يكون على وعي تام بالأساليب العلمية والفنية[61] التي تُستخدم في استخلاص الأدلة الرقمية. وبناءً عليه فإنه لجمع

---

[58] محمد عبيد سيف سعيد المسماري.(2007). الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية: دراسة تطبيقية مقارنة . بحث مقدم في المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، الرياض : جامعة نايف العربية للعلوم الأمنية، ص35 - 36.

[59] Rogers, C.(2013). Digital Records Forensics, p 16. See also: Ganesh, V. (2015). Digital Forensics, p 909.

[60] محمد حسين منصور . (2006). الإثبات التقليدى والإلكترونى . الأسكندرية : دار الفكر الجامعى، ص254 .

[61] لمزيد من التفاصيل حول الوسائل الفنية المستخدمة في جمع الوثائق (الأدلة) الرقمية، انظر: حسناء على على عبد الغني . (2022). علم الوثائق (الدبلوماتيك) وعلاقته بعلم الإثبات الجنائي الرقمي: دراسة نظرية وتطبيقية مقارنه. " أطروحة دكتوراه"، جامعة الأزهر ، ص 36 – 38.

الوثائق (الأدلة) في مجال الجرائم المعلوماتية بمعرفة الخبير المعلوماتي، يجب مراعاة القواعد الفنية المتعارف عليها في مجال الخبرة المعلوماتية، وتشـمل القواعد الفنية خطوات اشـتقاق الـدليـل الرقمي، والتي تتمثـل في خطوات مـا قبـل التشـغيـل والفحص وخطوات التشـغيـل والفحص[62] وتحديد مدى الترابط بين الدليل المادي والرقمي ومرحلة تدوين النتائج واعداد التقارير، **وتتمثل هذه القواعد فيما يلي:**

- جمع مجموعة من الأدلة الرقمية وتحصيلها من خوادم المواقع ومن جهاز الجاني.
- فحص الوثائق (الأدلة) الرقمية لمعرفة كيفية إعدادها ونسـبتها وتحديد عناصـر حركتها، ثم التوصل في النهاية إلى معرفة بروتوكول الإنترنت IP للحاسب الذي صدرت منه الرسائل والهجمات الإلكترونية، ومن خلال عنوان IP يمكن الحصـول على كل المعلومات الخاصـة بمزود الخدمة[63].

ويمكن ايجاز خطوات اشتقاق الدليل بمعرفة الخبير المعلوماتي فيما يلي:

خطوات مـا قبـل التشـغيـل والفحص: يجـب على الخبير أن يقوم بمـا يلي قبـل التشـغيـل والفحص:

- عمل نسـخة مطابقة للأصل لوسـائط التخزين المضبوطة كالقرص الصلب للقيام بعملية الفحص المبدئي وحماية الأصل من الفقدان أو التلف.
- التأكد من مطابقة محتوى الأحراز المضبوطة أثناء التحقيق بما هو مدون عليها.
- التأكد من صلاحية النظام للتشغيل.
- تسـجيل محتوى بيانات وحدات المكونات المضـبوطة، كالنوع والطراز أو الموديل، والرقم المسلسل[64].

---

[62] عبد الفتاح بيومي حجازي . (2003). الإثبات في جرائم الكمبيوتر والإنترنت. القاهرة: دار الكتب القانونية، ص187.

[63] خالد ممدوح إبراهيم . (2009). فن التحقيق الجنائي في الجرائم الإلكترونية. ط1. الأسكندرية: دار الفكر الجامعي، ص280، 300.

[64] معمش زهية، غانم نسيمة. (2013). الإثبات الجنائي في الجرائم المعلوماتية. "أطروحة ماجستير"، جامعة عبد الرحمن ميرة (بجاية)، ص 41. انظر أيضاً:

Duranti, L. (2009). From digital diplomatics, p63.

خطوات التشغيل والفحص:

- استكمال تسجيل باقي بيانات الوحدات من خلال قراءة جهاز الحاسب الآلي.
- تحديد أنواع وأسماء البرمجيات، كبرامج نظام التشغيل، وبرامج التطبيقات، وبرامج الإتصالات، وما إذا كان هناك برامج معينة ذات دلالة بموضوع الجريمة مثل برامج إنشاء ومعالجة الصور في جرائم التزييف والتزوير، والمونتاج.
- تحديد ما إذا كانت هناك مستندات أو معلومات ذات دلالة بموضوع الجريمة، كبصمات الأصابع بجرائم التزوير، ووجود رسائل التهديد في صندوق الصادر في البريد الإلكتروني .
- إظهار الملفات أوالنصوص المخبأة داخل الصور.
- تحويل الدليل الرقمي إلى دليل مادي عن طريق طباعة الملفات أو تصوير محتواها إذا كانت صوراً أو نصوصاً، أو وضعها في وعاء آخر حسب نوع البيانات والمعلومات المكونة للدليل.

جميع هذه الخطوات يمكن أن تتم بنجاح على الأصل، لكن لكي يتم استرجاع الملفات التي تم محوها من على الأصل، يجب اتباع الآتي:

- استخدام أحد برامج استعادة البيانات، وكذلك بالنسبة للملفات المعطلة أوالتالفة، وهذه البرامج متوافرة حتى للعامة مثل برنامج Easy Recover 4 all Professional، وتحرص الجهات المختصة دائماً على استخدام أحدث البرامج.
- تخزين هذه الملفات، أو البيانات، وعمل نسخ طبق الأصل أخرى من الإسطوانة أو القرص المحتوى لها، لفحصها عن طريق تطبيق الخطوات السابقة التي تمت على النسخ طبق الأصل.

تحديد مدى التر ابط بين الدليل المادي والدليل الرقمي

في هذه المرحلة يتم فحص كل من الدليل المادي المضبوط، والدليل المادي المستخرج من جهاز الحاسب الآلي (أصل الدليل الرقمي) الموجود بملفات النظام المضبوط (صور – نصوص – أصوات)، وبذلك يكون قد تم الربط بين الدليل الرقمي والدليل المادي، مما يكسب الدليل الموثوقية، واليقين، اللتان تمنحانه الحجية أمام المحكمة[65]. ومن الجدير بالذكر أنه

[65] محمد عبيد سيف سعيد المسماري.(2007). الإثبات الجنائي بالأدلة الرقمية، ص35 - 36.

أثناء الفحص ينبغي إعداد الصور الفوتوغرافية والمطبوعات والرسوم البيانية وغيرها من البيانات أو الوثائق التي تدعم النتائج والاحتفاظ بها، كما ينبغي توثيق كافة الإجراءات الفنية والإدارية على حد سواء[66].

(4) مرحلة تدوين النتائج وإعداد التقرير:

في هذا النشاط, يقوم المحقق الجنائي بإعداد تقرير موقع منه لما توصل إليه من نتائج من بداية إجرائه للتحقيق، وغالباً ما يُرفق به الملاحق الإيضاحية المصورة أو المسجلة، لاعتمادها ثم تقديمها إلى جهة التحقيق أو الحكم[67].

(5) تقديم حزمة الأدلة:

يقوم المحقق الجنائي بتقديم كل الوثائق والتقارير إلى الفريق القانوني أو فريق المحققين لإرفاقها مع المواد التي سوف يتم تقديمها للمحكمة أو الجهة القانونية المختصة [68]. وتتمثل أهمية هذه المرحلة في تقديم وعرض النتائج التي تم التوصل إليها من إجراء التحقيقات الفنية وفي الغالب يشهد إجراء تحقيق وتقديم الدليل كل من الشرطة والنيابة والمتهم ومحاميه والقاضي، ولكن يجب أن يقوم جهاز الشرطة بتقييم الدليل مسبقاً قبل عرضه أمام المحكمة[69].

(6) إدارة مواد القضية:

النشاط الأخير الذي يتم اتخاذه كجزء من التحقيقات هو إدارة مواد القضية. وفقا للمتطلبات القانونية, فإن حفظ وتنظيم المواد قد يشمل تخزين مواد القضية, أو التخلص منها Destruction, وإعادة الممتلكات العينية (المادية)لأصحابها الأصليين[70].

يتضح مما سبق، أن أسس السلطة التي يتمتع بها خبراء الدبلوماتيك الرقمي وخبراء الأرشيف وخبراء الأدلة الجنائية الرقمية تنبع من النظرة الخاصة المهمة لجودة الدليل الذي يسعون هم للتحقق من صحته. وبالرغم من اختلاف وجهات نظرهم بخصوص تحليل المواد الرقمية, إلا أن أهدافهم واحدة, وهي: التحقق من الأدلة الرقمية على الأحداث والفعاليات

---

[66] Duranti, L. (2009). From digital diplomatics, p63.

[67] معمش زهية، غانم نسيمة. (2013). الإثبات الجنائي في الجرائم المعلوماتية، ص 41.

[68] Rogers, C.(2013). Digital Records Forensics, p 16.

[69] ممدوح عبد الحميد عبد المطلب.(2003). أنموذج مقترح لقواعد اعتماد الدليل الرقمي، ص 2248 .

[70] Rogers, C.(2013). Digital Records Forensics, p 16.

وإثبات صحتها. ومن هذا المنطلق, يتوجب على المحققين من كلا المجالين تثبيت وتوثيق هوية وسلامة وسياق الدليل, والاستعداد لتبريره أو تفسيره, وكذلك شرح دورهم في كشفه ووصفه. لأنه من المحتمل وجود تقاطع بين مفهومي الدبلوماتيك وعناصر التحقيق الجنائي[71].

ثالثاً - خطوات تطبيق النقد الدبلوماتي الرقمي على نماذج من الوثائق (الأدلة) الرقمية للجر ائم المعلوماتية لمحكمة القاهرة الاقتصادية:

تنبه المُشرع المصري لمبدأ التخصص القضائي فأنشأ المحاكم الإقتصادية الجنائية بموجب القانون رقم 120 لسنة 2008، لتختص دون غيرها بنظر منازعات بعينها، وتكمن فكرة إنشاء المحاكم الإقتصادية في أنها محاكم مخصصة للفصل في المنازعات التجارية والاستثمارية، أُنشئت مواكبة لمرحلة الإصلاح الإقتصادي، الذي يستهدف تحرير التجارة ودعم الاستثمار وجذب المزيد من المستثمرين، بهدف إزالة المعوقات المؤثرة على كفاءة الأداء الإقتصادي، وسرعة حسم الدعاوى الإقتصادية المنظورة أمام القضاء(72). ولأن المحكمة الاقتصادية في مصر هي المختصة بنظر الدعاوى الجنائية الناشئة عن الجرائم المعلوماتية فقد اعتمدت الباحثة في تطبيق منهج علم الوثائق (الدبلوماتيك) الرقمي على نماذج من الملفات القضائية للجرائم المعلوماتية لمحكمة القاهرة الاقتصادية.

والجدول رقم (1) يوضح نماذج الجرائم المعلوماتية التي تم التطبيق عليها:

رقم القضية	نوع الو اقعة (الجريمة)	الوصف القانوني للو اقعة
2569 لسنة 2009	تزوير بطاقة الائتمان	جنح
113 لسنة 2019	اختراق البريد الإلكتروني	جنح
844 لسنة 2013	تزوير البريد الإلكتروني	جنح
307 لسنة 2017	سرقة حساب الفيس بوك	جنح
271 لسنة 2019	رسالة واتساب تتضمن عبارات سب وتهديد للمجني عليها	جنح

(71) Rogers, C.(2013). Digital Records Forensics, p 9.

(72) أيمن رمضان الزيني. (2015). المحاكم الإقتصادية ودورها في تشجيع الاستثمار. دراسة مقدمة إلى مؤتمر القانون والاستثمار، جامعة طنطا، ص1. متاح على الرابط التالي: https://law.tanta.edu.eg/files/pdf (last visited 9/11/2020).

1- التعريف بالمحكمة الإقتصادية (جهة منشأ الوثائق):

هي نوع من المحاكم المتخصصة تختص نوعياً ومكانياً بقوانين محددة، وقد تم إستحداثها وإنشاؤها بموجب القانون رقم 120 لسنة 2008 الخاص بإنشاء المحاكم الاقتصادية وهو التشريع الذي يحدد اختصاصاتها وتشكيلها، كما ينظم كافة المسائل المتعلقة بها، وتم العمل بهذا القانون اعتبارا من الأول من أكتوبر سنة 2008، كما تم تعيين مقر محكمة القاهرة الإقتصادية بموجب قرار السيد وزير العدل رقم 8603 لسنة 2008 والخاص بتحديد مقار المحاكم الإقتصادية على مستوى الجمهورية، حيث توجد في مصر ثمانٍ محاكم اقتصادية[73].

تشكيل دوائر محكمة القاهرة الاقتصادية:

تتشكل المحكمة الاقتصادية من دوائر ابتدائية ودوائر استئنافية، ويصدر بتعيين مقار هذه الدوائر قرار من وزير العدل بعد أخذ رأى مجلس القضاء الأعلى. كما أنَ هناك هيئة لتحضير المنازعات والدعاوى التي تختص بها هذه المحكمة، وجدول لخبراء المحكمة الإقتصادية. وتُشكل كل دائرة من الدوائر الابتدائية الاقتصادية من ثلاثة من الرؤساء بالمحاكم الإبتدائية، وتُشكل كل دائرة من الدوائر الاستئنافية من ثلاثة من قضاة محاكم الإستئناف يكون أحدهم على الأقل بدرجة رئيس بمحكمة الإستئناف[74].

وتنعقد الدوائر الابتدائية والاستئنافية المنصوص عليها في الفقرة السابقة في مقار المحاكم الاقتصادية، ويجوز أن تنعقد، عند الضرورة، في أي مكان آخر وذلك بقرار من وزير العدل بناء على طلب رئيس المحكمة الاقتصادية.

وتعين الجمعية العامة للمحكمة الاقتصادية، في بداية كل عام قضائي، قاضيا أو أكثر من قضاتها بدرجة رئيس بالمحاكم الابتدائية من الفئة (أ) على الأقل، ليحكم، بصفة مؤقتة، ويختص قاضي الأمور الوقتية بالفصل في المسائل المستعجلة التي يخشى عليها من فوات الوقت والتي تختص بها تلك المحكمة شريطة توافر أمور ثلاث:

- أن تكون المنازعة المستعجلة داخلة في نطاق المنازعات التي تختص بها المحكمة الاقتصادية.

---

[73] وزارة العدل. (2009). دليل إجراءات التقاضي لدى المحاكم الإقتصادية، ص7 - 8. متاح على الرابط التالي: http://www.jp.gov.eg/ar/LS.pdf (last visited 9/2/2020).

[74] راجع نصي المادة (1/2)، (2/2) من قانون إنشاء المحاكم الإقتصادية رقم 120 لسنة 2008.

- ألا يترتب على الفصل فيها المساس بأصل الحق.
- أن يكون فصله في المنازعات بصفة مؤقتة وليس موضوعية[75].

اختصاص محكمة القاهرة الاقتصادية:

تختص المحاكم الإقتصـادية بالفصـل في الدعاوى الجنائية والمدنية الإقتصـادية، ويتحدد اختصاصها وفقاً للقواعد التالية:

- تختص الدوائر الابتدائية بنظر الجُنح كمحكمة أول درجة بديلاً عن المحكمة الجزئية والقاضي الفرد.
- تختص الدوائر الاسـتئنافية بنظر الطعن في الأحكام الصـادرة في الجنح، وهو الدور الذي تقوم به محكمة الجُنح المستأنف في المحاكم الابتدائية[76].

2 - تطبيق عناصـر النقد الدبلوماتي الرقمي على الوثائق (الأدلة) الجنائية الإلكترونية للجر ائم المعلوماتية:

تتمثل أوجه التشـابه بين منهج علم الإثبات الجنائي الرقمي ومنهج علم الدبلوماتيك الرقمي في تقييم أصـالة وتحديد سـياق ومصـدر وعلاقات ومعنى الوثائق (الأدلة) الرقمية. كما تظهر أوجه التطابق بين المنهجين من خلال فحص المصـدر أو نقد المصـدر، حيث يبدأ النقد (الفحص) الدبلوماتي للوثائق (الأدلة) الجنائية بنقد المصـدر أو فحص المصـدر وكذلك في الإثبات الجنائي تبدأ عملية الإثبات بفحص مصـدر الوثيقة. وبناءً عليه سـوف يتم تطبيق عناصـر النقد الدبلوماتي الرقمي على الوثائق (الأدلة) الجنائية الإلكترونية لنماذج من الجرائم المعلوماتية، ومن ثم توضيح أوجه التطابق والإختلاف بين المنهجين.

الجريمة الأولى: جريمة تزوير محرر إلكتروني (بطاقة الائتمان أو كارت الفيزا)

بطاقات الائتمان هي بطاقات تصـدر بمعرفة مؤسـسـة مالية أو بنك باسـم أحد الأشخاص وتؤدي وظيفتي الوفاء والائتمان، أي أنها تعطي لحاملها الحق في متابعة سداد المبالغ التي استخدمها من الاعتماد المفتوح لدى مصدر البطاقة[77].

---

[75] أيمن رمضان الزيني. (2015). المحاكم الإقتصادية ودورها في تشجيع الاستثمار، ص 24-25.

[76] وزارة العدل. (2009). دليل إجراءات التقاضي لدى المحاكم الإقتصادية، ص9.

[77] ثناء أحمد محمد المغربي.(2003).الوجهة القانونية لبطاقات الائتمان. دراسه مقدمه إلى مؤتمر الأعمال المصرفيه الإلكترونيه بين الشريعه والقانون, مجموعة أعمال المؤتمر, المجلد الخامس, الإمارات العربيه المتحده، ص945.

إن جريمة الإعتداء بالتزوير على التوقيع الإلكتروني لبطاقات الائتمان من أكثر الجرائم الإلكترونية خطورة لمساسها بالذمة المالية لصاحب البطاقة وإضعاف الثقة في البنوك المصرفية، ورغم الحماية التقنية العالية التي تتميز بها الأرقام السرية، إلا أن الإجرام أيضاً متطور ويتماشى مع التطور التكنولوجي للأنظمة الإلكترونية المصرفية، مما زاد عمليات التلاعب في التوقيع الإلكتروني[78]. ويُعتبر هذا النوع من الجرائم من أشهر القضايا التي واجهتها مصر في بداية عام 2003، حيث تم استغلال أرقام بطاقات الإئتمان الشخصية للشراء عبر الإنترنت.

التحليل الدبلوماتي الرقمي لبطاقات الائتمان كوثيقة تفاعلية غير ديناميكية:

نظراً لأن بطاقات الائتمان تعتبر مصدراً خصباً وغنياً للأدلة التفاعلية غير الديناميكية التي يمكن أن تستخدم في الإجراءات الجنائية، لذلك وفقاً للدبلوماتيك الرقمي قبل الشروع في استخراج عناصر النقد يجب فحصها أولاً للتأكد من كونها وثيقة أم لا، وذلك بالبحث عن المكونات الست للوثيقة (بطاقة الائتمان):

أولاً- المحتوى:

يشترط علم الوثائق (الدبلوماتيك) الرقمي أن يكون الكيان الرقمي له شكل ثابت ومحتوى مستقر حتى يكون وثيقة أرشيفية، واعتبرهما أهم مكونات الوثيقة الدبلوماتية[79]. وتعتبر بطاقات الائتمان نموذجاً للوثائق التفاعلية غير الديناميكية، حيث ترتبط بطاقات الائتمان بالتوقيع الإلكتروني ارتباطاً وثيقاً لأنه لا يمكن أن تتم أي عملية للبطاقة إلا عن طريق التوقيع الإلكتروني وبواسطته يتأكد النظام الإلكتروني المصرفي للبنك من هوية صاحب التوقيع، أي أنَ بطاقات الائتمان تُتيح التفاعل بين مالك البطاقة وبين النظام المعلوماتي للبنك المُصدر لها[80].

كما تعتبر بطاقات الائتمان صورة حديثة لعملية التوقيع الإلكتروني لأنها تحمل بيانات تكون بمثابة المفتاح العام وشريط ممغنط يحتوي على بيانات إلكترونية تكون بمثابة

---

[78] فارس خطابي. (2020). تزوير التوقيع الإلكتروني في بطاقات الائتمان: دراسة على ضوء القانون 15 – 4 المتعلق بالتوقيع والتصديق الإلكترونيين. المجلة الجزائرية للأمن الإنساني، 5 (2)، ص 665.

[79] دينا محمود عبد اللطيف. نفس المرجع، ص 357.

[80] فارس خطابي. (2020). نفس المرجع، ص 655.

المفتاح الخاص ولا يستطيع صاحب البطاقة أو الكارت سحب أي مبلغ نقدي بواسطته إلا إذا أدخل الكارت في ماكينة سحب النقود وأدخل بعد ذلك الرقم السري الذي لا يعرفه أحد سواه، وبدون الكارت والرقم السري لا ينتج الكارت أي أثر، وبهذه الصورة يعتبر هذا الكارت بمثابة توقيع إلكتروني، لأن البنك بناءً عليه يُعطي أو يصرف النقود التي يريدها صاحب الكارت في حدود حسابه[81]، وهذا ما يجرى عملياً في حالة استخدام بطاقات الائتمان، وهي إحدى صور التوقيع الإلكتروني الكودي التي كثُر التعامل بها في نظم المعالجة الإلكترونية. فإدخال العميل الرقم السري بنفسه يُعد في حد ذاته توقيعاً إلكترونياً ودليلاً على أنه صدر منه شخصياً في صورة لأرقام سرية لا يعرفها إلا هو[82]. تعمل بطاقة الائتمان الممغنطة بنظامي الاتصال المباشر (On Line) ونظام الاتصال غير المباشر (Off Line). كما تحتوى بطاقات الائتمان على مجموعه من البيانات الظاهرة للعين المجردة، هذه البيانات تُحدد الجهة المُصدرة لها وهوية الشخص حاملها والتاريخ المسموح به استخدامها من قبل حاملها[83].

من خلال ما سبق، يتضح أن القواعد التي تحكم عرض المحتوى في بطاقات الإئتمان ثابته لا تتغير، وبناءً عليه يمكن القول أن بطاقة الائتمان ذات محتوى مستقر.

ثانياً - الشكل

يتكون الشكل الثابت من جميع جوانب الشكل الذي يقوم بتحديده البنك المُصدر للبطاقة، ويشمل ثبات الشكل في بطاقات الائتمان جميع الجوانب التي تظهر دائماً في البطاقات مهما تغير المحتوى، فهي عبارة عن بطاقات بلاستيكية مصنوعة من مادة خاصة مستطيلة الشكل يظهر على أحد وجهيها الأمامي بيانات رقمية تظهر بأحرف بارزة، تحدد الجهة المصدرة لها، وهوية الشخص حاملها، ونطاق صلاحيتها، واسم الشركة العالمية للبطاقة وشعارها. وعلى الوجه الخلفي يوجد شريط البيانات الممغنط، مخزن عليه جميع البيانات المشفرة الخاصة بحاملها والخاصة بالبنك المصدر لها. كما يوجد توقيع إلكتروني مشفر على ظهر البطاقة، بالإضافة إلى رمز الأمان الخاص بالبطاقة[84].

---

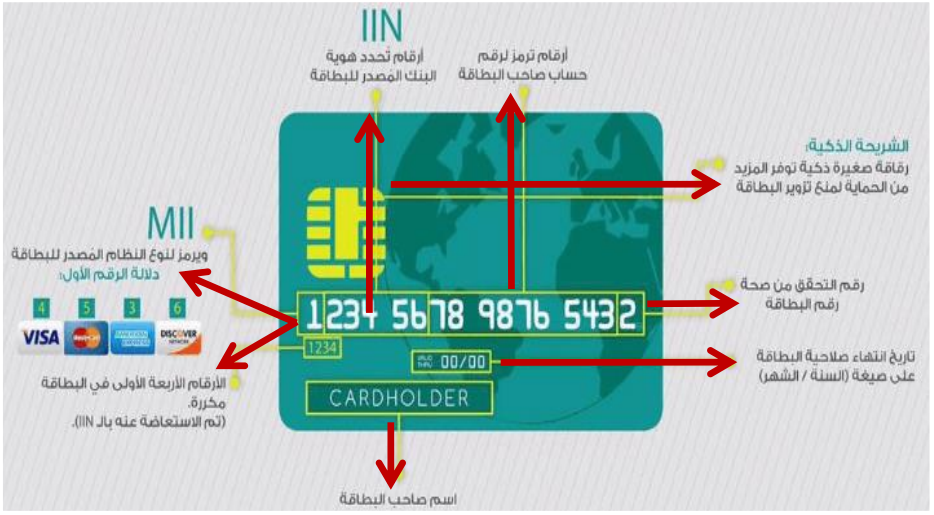
[81] أيمن سعد سليم. (2004). التوقيع الإلكتروني: دراسة مقارنة. القاهرة: دار النهضة العربية، ص28.

[82] نجوى أبو هيبة. (2001). التوقيع الإلكتروني – تعريفه – مدى حجيته في الإثبات. دراسه مقدمه إلى مؤتمر الأعمال المصرفيه الإلكترونيه بين الشريعه والقانون, مجموعة أعمال المؤتمر, المجلد الخامس, الإمارات العربيه المتحده، ص447 – 448.

[83] ثناء أحمد محمد المغربي.(2003).الوجهة القانونية لبطاقات الائتمان، ص946.

[84] ثناء أحمد محمد المغربي.(2003).الوجهة القانونية لبطاقات الائتمان، ص946.

وتشـــتمل جميع بطاقات الائتمان على رقم مميز وخاص لكل بطاقة مكون من ســـتة عشـر رقماً يتم طباعته أو نقشـه على الوجه الأمامي للبطاقة الخاصـة بالعميل كما هو موضح في الشكل رقم (4)، وهذه الأرقام الستة عشر تتآلف من أربعة أقسام كل قسم يتآلف من أربعة أرقـام وفقـاً للمعيـار الـدولي لترقيم البطـاقـات الائتمـانيـة ISO/IEC 7812. القســـم الأول من البطاقـة خـاص برقمIIN ، وهو عبـارة عن عـدد من الأرقـام والتي يتم من خلالهـا تحـديـد هويـة البنك الذي يقوم بإصـــدارها، والرقم الأول منها MII يرمز لنظام مصـــدر البطاقة، حيث يوجد أربع شـركات رئيسـة تقوم بصـرف بطاقات الائتمان، وهي فيزا Visa وماسـتركارد Master Card وأمريكان اكســـبريس AMEX، وديســـكفر Discover . أما القســـم الثالث من أرقام بطاقة الائتمان عبارة عن أرقام تُشـير إلى الحسـاب الخاص بصـاحب البطاقة ويُشـير الرقم الأخير من أرقام بطاقة الائتمان إلى الرقم الذي يُســـتخدم للتحقق من صـحة البطاقة. كما توجد أربعة أرقام أسـفل رقم البطاقة تدل على تاريخ انتهاء صلاحية البطاقة (سـنة / شـهر) وفي أسـفل وجه البطاقة اسم صاحب البطاقة [85].



شكل رقم (4) يوضح الوجه الأمامي لبطاقة الائتمان

[85] ISO/IEC 7812-1:2017 specifies a numbering system for the identification of the card issuers, the format of the issuer identification number (IIN) and the primary account number (PAN), p2.

يتضح مما سبق، أن القواعد التي تحكم عرض المحتوى والشكل لبطاقات الائتمان ثابتة لا تتغير، أي أن بطاقات الائتمان ذات شكل ثابت ومحتوى مستقر.

ثالثاً - الحدث

لابد للوثيقة أن تُشارك في حدث ما، وبطاقات الائتمان تُشارك بوجه عام فيما يُطلق عليه السداد الإلكتروني، ولا يعني ذلك أن وظيفة البطاقة تقتصر فقط على السداد، بل إنَ لها وظائف أخرى لكونها آداة ائتمان أو وسيلة لسحب النقود[86].

رابعاً - الأشخاص

أطراف البطاقة:

- **مصدر البطاقة:** هو المؤسسة أو البنك الذي يصدر البطاقة للعميل بناءً على ترخيص معتمد من المنظمة العالمية بصفته عضواً فيها، وهو الذي يُسدد وكالة عن حامل البطاقة قيمة المشتريات للتاجر.
- **حامل البطاقة:** هو الشخص الذي صدرت البطاقة باسمه، أو خول باستخدامها، والتزم لمصدر البطاقة بالوفاء بكل ما ينشأ عن استعماله البطاقة، فحامل البطاقة قد يكون هو الشخص الذي صدرت البطاقة باسمه، وقد يكون هو الشخص الذي يستخدم البطاقة بناءً على تفويض من صاحبها.
- **التاجر الذي يقبل البطاقة:** التاجر هو الذي يتعاقد مع مصدر البطاقة على تقديم السلع والخدمات الموجودة عنده عندما يطلبها حامل البطاقة من البنك الذي تم الإتفاق معه.
- **المنظمات الراعية للبطاقة:** توجد عدة منظمات ترعى البطاقات أشهرها، منظمة الفيزا، ومنظمة الأمريكان اكسبرس[87].

خامساً -السياق

1 - السياق القانوني لبطاقات الائتمان: تعمل بطاقات الائتمان وفقاً لقوانين حماية البيانات الشخصية للمستخدمين وقوانين أمن المعلومات مثل قوانين التوقيع الإلكتروني وقوانين مكافحة الجرائم المعلوماتية.

---

[86] فارس خطابي. (2020). نفس المرجع، ص 655.

[87] الصديق محمد الأمين الضرير. (2003). بطاقات الائتمان. دراسه مقدمه إلى مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون, مجموعة أعمال المؤتمر, المجلد الخامس, الإمارات العربيه المتحدة، ص 640 - 641.

2 - **سـياق المصـدر:** ظهرت بطاقات الائتمان كفكرة قامت بها بعض المؤسـسـات والمحلات التجارية الكبرى، ومكاتب الرحلات السياحية وشركات البترول في الولايات المتحدة الأمريكية في الفترة من 1945 – 1948، وكان هدفها ضـمان إخلاص واسـتمرار عملائها في تعاملهم معها، وذلك من خلال منحهم تسـهيلات في الوفاء، وكانت هذه البطاقات لا تقبل إلا لدى فروع هذه المنشـآت. وفي عام 1949 تم إصـدار بطاقة شـركة Diners Club وتعني (نادي الطاعمين)، ثم ظهرت بطاقة American Express Card))عام 1958م لتمكن حاملها من اسـتفادة الحصـول على السـلع والخدمات من الفنادق والشـركات، على أن تحصـل من عملائها ما يضـمن اسـترداد ما تقوم بدفعه لحسـاب فواتيرهم. ثم توالت البنوك في أمريكا عام 1958 بالدخول إلى ميدان بطاقات الائتمان، ولخطورة هذه الوسـيلة الجديدة من وسـائل الدفع على التعاملات التجارية، قامت البنوك باسـتخدام خبراتها المصـرفية لتطوير هذه الوسـيلة ورعايتها، ثم ظهر بعد ذلك التاريخ مؤسـسـات خاصـة ببطاقات الائتمان مثل مؤسستي Master Card ، Visa Card الأمريكيتين. وفي عام 1967 انتقل التعامل ببطاقات الائتمان إلى أوروبا، فصـدرت بطاقات الائتمان عن بنوك ومؤسـسـات مالية لأول مرة في فرنسا، ومن أشهرها (Cartes Du Diners)، ويُعتبر ذلك هو مصدر بطاقات الائتمان [88].

3 - **السـياق التوثيقي:** ترتبط بطاقة الائتمان بالنظام المعلوماتي للبنك المصدر لها، كما يرتبط النظام المعلوماتي للبنك المصدر للبطاقة بالنظام المعلوماتي للتاجر، حيث يستطيع التاجر الحصـول على موافقة البنك على إتمام العملية من خلال نظام الربط الإلكتروني بينهما. وقد تطورت العملية إلكترونياً الآن بفضـل أجهزة الربط الإلكتروني ما بين نقاط البيع والبنوك، بحيث يقوم التاجر بتمرير البطاقة عبر جهاز إلكتروني[89] في نقطة البيع ومن ثم يدخل قيمة العقد، فيحصـل اتصـال إلكتروني بموجبه تقيد العملية على حسـاب البنك

---

[88] علي جمال الدين عوض. (1988). عمليات البنوك من الوجهة القانونية. القاهرة: دار النهضة العربية، ص 429.

[89] هو جهاز يمكنه فك شفرة المعلومات الموجودة في الشريط الممغنط أو الرقاقة الممغنطة لبطاقة الائتمان أو بطاقة الخصم. يسمح قارئ البطاقات للعملاء بالوصول إلى حساباتهم البنكية من خلال ماكينات الصراف الآلي ويسمح للمستهلكين بإجراء عمليات الشراء باستخدام بطاقات الائتمان والخصم. انظر: ممدوح بن رشيد الرشيد العنزي. (2015). الحماية الجنائية لبطاقات الدفع الإلكتروني من التزوير. المجلة العربية للدراسات الأمنية والتدريب، 31 (62)، ص47.

الذي صـدرت عنه البطاقة التي تعود لحاملها، وبعد ذلك وإضـافة لعملية الإثبات يصـدر إشعار بالعملية يتم توقيع صاحب البطاقة عليه، وبمجرد الحصول على الموافقة إلكترونياً، يتم قيد المبلغ من حسـاب صـاحب البطاقة إلى حسـاب التاجر[90]. وتمثل هذه الخطوات السياق التوثيقي لبطاقات الائتمان.

4 - **السـياق التقني:** يُقصـد بالسـياق التقني وفقاً للدبلوماتيك الرقمي أنه المكونات التقنية للنظام الذي أنشـأ الوثيقة، والمكونات المادية (مثل وسـيط التخزين)، والبرمجيات (مثل نظام التشـغيل، برمجيات النظام، البرامج التطبيقية، برمجيات الشـبكة)، البيانات التي تشمل هيكل الملف والعلاقات بين الملفات داخل النظام وبيانات عن صيغة الملف أو تنظيم البيانات داخل الملفات مثل معلومات عن إدارة النظام)[91]. ويُقصـد به هنا البيئة التقنية للنظام الذي أنشأ بطاقات الائتمان.

تعمل بطاقة الائتمان الممغنطة بنظامين: نظام الاتصال المباشر (On Line) ونظام الاتصال غير المباشر (Off Line) يسمح النظام الأول بالخصم الفوري من حساب العميل، فهو أكثر تطوراً من الثاني الذي يكون فيه الخصـم مؤجلاً[92]. هذه البطاقة تكون مزودة أيضـاً بمعالج بيانات صـغير الحجم، يتضـمن القيمة المالية التي يسـتطيع حاملها إنجاز معاملاته في حدودها. كما يوجد لكل بطاقة ائتمان شـريط ممغنط وهو مصـنوع من ذرات حديدية ممغنطة تُسـتخدم لتخزين المعلومات وقراءتها في أجهزة القارئ في نقاط البيع[93]. يُقسم الشريط إلى ثلاث مسارات كما هو موضح في الشكل رقم (5): الأول لتخزين معلومات البطاقة وصـاحبها والبنك المصـدر لها وغيرها. أما المسـار الثاني فخاص بتخزين نفس المعلومات الموجودة في المسار الأول ولكن بصيغة مختلفة عن المستخدمة في المسار الأول أما المسـار الثالث فهو خاص بالقراءة والكتابة على البطاقة ويتم به تخزين المعلومات التي قد تتغير مثل الرقم السري للبطاقة (PIN) وغيرها.

---

[90] عمر عبد السلام حسين الجبوري.(2017). جريمة التزوير الإلكتروني في التشريع الأردني: دراسة مقارنة. "أطروحة ماجستير"، جامعة الشرق الأوسط، ص 31 – 32.

[91] دينا محمود عبد اللطيف. نفس المرجع، ص302 – 303.

[92] عبد الجبار الحنيص. (2008). الحماية الجزائية لبطاقات الائتمان الممغنطة من التزوير. مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، 24(2)، ص 149.

[93] عبد الجبار الحنيص. (2008). مرجع سابق، ص 149، 164.

رمز الأمان:

هو عبارة عن رمز إضافي مطبوع على بطاقة الائتمان والسحب الآلي الخاصة بالمستخدم. وفي معظم البطاقات (Visa و Master Card والبطاقات الصادرة عن البنوك وغيرها)، يكون ذلك الرمز هو آخر ثلاثة أرقام مطبوعة على شريط التوقيع الموجود على ظهر البطاقة الخاصة بالمستخدم. أما على بطاقات (أمريكان إكسبريس AMEX) فعادةً ما يكون عبارة عن رمز مؤلف من أربعة أرقام موجود على وجه البطاقة . ونظرًا لأن رمز CVC لا يكون بارزًا (عكس رقم البطاقة)، فإنه لا تتم طباعته على أي من الإيصالات، وبالتالي فليس من المرجح أن يعرفه أي شخص بخلاف صاحب البطاقة. على سبيل المثال، عند إدخال تفاصيل بطاقة الائتمان في موقع للقيام بالشراء باستخدامها، فالموقع يطلب من المستخدم كتابة رمز أو رقم التحقق (CVC) لأسباب أمنية. ويتم تحويل كل المعلومات التي يرسلها المستخدم عبر اتصالات SSL الآمنة [94].

شكل رقم (5) يوضح الوجه الخلفي لبطاقة الائتمان

سادساً - الرابطة الأرشيفية

يجب أن تحتوي الوثيقة (بطاقة الائتمان) على رابطة أرشيفية، وهي العلاقة التي تربط كل وثيقة بالوثيقة السابقة واللاحقة لنفس الإجراء، وبصورة تدريجية، إلى جميع الإجراءات التي تُشارك في نفس النشاط. وهذا يعني أن كل أصل رقمي يشكل رابطة فكرية مع كل أصل رقمي آخر. والمقصود بالرابطة الأرشيفية هنا رقم بطاقة الائتمان الموجود على الوجه الأمامي للبطاقة.

[94] ممدوح بن رشيد الرشيد العنزي. (2015). نفس المرجع، ص47، 56 .

يتضح من خلال ما سبق، أن بطاقات الائتمان قد استوفت جميع متطلبات الوثيقة على النحو المحدد في مشروع الانتربارس (شكل ثابت ومحتوى مستقر والأشخاص والحدث والسياق والرابطة الأرشيفية)، ولذلك يمكن الحكم على بطاقات الائتمان أنها وثائق دبلوماتية تستحق النقد من علم الدبلوماتيك لكي يكون لها حجية أمام القضاء.

عناصر النقد الدبلوماتي الرقمي لبطاقة الائتمان أو الفيزا موضوع الجريمة

تتلخص وقائع هذه القضية في قيام المتهم بتزوير محرر إلكتروني (بطاقة الائتمان أو كارت الفيزا)، بالإضافة إلى استعمال البطاقة الإلكترونية المزورة في شراء سلع ومنتجات من محلات جاب الله وحيازته لعملات مقلدة وللبطاقة الإلكترونية المزورة الثانية المضبوطة[95].

- السياق

يُشير السياق وفقاً لعلم الوثائق (الدبلوماتيك) إلى مجموعة الظروف والأحوال التي تحيط بالوثيقة أو الحدث، وفحص السياق يُعزز من قيمة الوثيقة ويُساعد في إثبات صحتها[96]. أما في مجال الإثبات الجنائي فيُقصد به الإطار القانوني والإداري الذي يتم فيه إجراءات الدعوى الجنائية.

1 - سياق المصدر[97]

يبدأ النقد (الفحص) الدبلوماتي للوثائق (الأدلة) الجنائية بنقد المصدر أو فحص المصدر وكذلك في الإثبات الجنائي تبدأ عملية الإثبات بفحص مصدر الوثيقة، وذلك بالبحث عن من هو الشخص المسؤول عن تزوير بطاقة الائتمان أو الفيزا، ثم التعرف على المصدر وتحديده من خلال رقم الحساب المطبوع على البطاقة. وقد يكون المصدر جهة أو شخص والمقصود بالمصدر هنا هو الشخص المسؤول عن تزوير بطاقة الائتمان أو الفيزا.

تبدأ عملية الإثبات الجنائي بعد قيام المتهم باستعمال بطاقة الفيزا المزورة في شراء جهاز تليفزيون من المحل الذي يعمل المجني عليه مسئولاً للبيع به، قام البائع بمضاهاة رقم بطاقة الفيزا بالرقم المطبوع على إشعار الخصم الذي خرج من ماكينة السحب وتبين وجود

---

[95] قضية جنحة رقم 2569 لسنة 2009 جنح اقتصادية القاهرة.

[96] دينا محمود عبد اللطيف محمد. (2017). الإتجاهات الحديثة فى علم الوثائق (الدبلوماتيك)، ص 230 .

[97] المصدر هو أصل الوثيقة ومحل إثبات صحتها، ويُقصد بسياق المصدر وفقاً لعلوم الحاسب الآلي كل مرحلة من مراحل دورة حياة الوثيقة، حيث أن السياق والتفاصيل الفنية توجد في إطار النشأة، كذلك البيانات التي تساعد في تقييم صحة المعلومات وتحديد الاستخدام المناسب لها تعتبر معلومات خاصة بالمصدر. انظر: دينا محمود عبد اللطيف محمد. (2017). نفس المرجع، ص302.

اختلاف بينهما، وبناءً عليه تم عرض الكارت على إدارة مكافحة جرائم التزييف والتزوير(وحدة البحوث الفنية) للفحص، وقد قامت الإدارة بمضاهاة رقم بطاقة الفيزا، والتي تحمل رقم 453978116759451 بالرقم المطبوع على إشعار الخصم الذي خرج من ماكينة السحب، والذي يحمل رقم 4640166004028665، وتبين وجود اختلاف بينهما، وهو ما يقطع بتزوير ذلك الكارت.غير أنه لم يتم تحديد المالك الفعلي لتلك البطاقة، لكن من خلال رقم الحساب المطبوع على البطاقة 453978116759451 تبين أنه منسوب لبنك نات ويست، وهو بنك تجاري كبير في المملكة المتحدة .

ويعتبر ما قامت به إدارة مكافحة جرائم التزييف والتزوير مطابقاً لمنهج علم الدبلوماتيك، غير أنه وفقاً لمنهج علم الدبلوماتيك كان يجب فحص الخصائص الداخلية والخارجية لبطاقة الائتمان، إلا أن إدارة مكافحة جرائم التزييف والتزوير اكتفت بمضاهاة رقم الحساب المطبوع على البطاقة بالرقم المطبوع على إشعار الخصم، وقد وُجد عدم توافق بين رقم البطاقة والرقم المطبوع على سجل المبيعات، الأمر الذي يقطع بتزوير الكارت، وهو ما يُسمى في الدبلوماتيك بعدم التوافق الداخلي نظراً لأن منهج الدبلوماتيك قائم على تحديد التوافق أو عدمه، فلو كانت بطاقة الائتمان صحيحة كان يجب أن يتوافق رقم البطاقة مع الرقم المطبوع على سجل المبيعات. كما أنه لتحديد مصدر الوثيقة (بطاقة الفيزا) وفقاً لمنهج علم الدبلوماتيك كان يجب فحص التوقيع الإلكتروني الموجود على بطاقة الائتمان، نظراً لأنه من الخصائص الخارجية للبطاقة والتي يمكن من خلالها تحديد هوية المالك الفعلي للبطاقة عن طريق الرجوع للبنك المصدر لها ومضاهاة ومقارنة البيانات المخزنة في البطاقة مع البيانات المماثلة المخزنة في قاعدة بيانات البنك المصدر لها حتى يتم نسبة البطاقة إلى صاحبها الحقيقي.

بالإضافة إلى أنه وفقاً لمنهج علم الدبلوماتيك كان يجب التحقق من توافق العناصر الداخليه والخارجية للبطاقة مع مثيلاتها الصادرة من نفس البنك المصدر لها حتى يمكن الحُكم بصحة هذه البطاقة أو تزويرها. ومن المعروف أن العناصر الداخلية والخارجية في البيئة الإلكترونية عبارة عن بيانات وصفية (ميتاداتا)، تضم معلومات سياقية تدعم محتوى الوثيقة أو موضوعها. فمن خلال تحليل عناصر الميتاداتا يمكن معرفة مظهر الوثيقة (بطاقة الائتمان) الخارجي، كما يمكن تحديد أسماء الأشخاص المسؤولين عن الحدث والموضوع الذي شاركت فيه، كذلك يمكن الكشف عن التناقضات في رقم الحساب المطبوع على الفيزا من خلال مقارنته مع الرقم المطبوع على إشعار الخصم الذي خرج من ماكينة السحب، الأمر الذي يقطع بالتزوير. والجدول رقم (2) يوضح ميتاداتا الهوية لبطاقة الائتمان المزورة:

ميتاداتا الهوية

عناصر الميتاداتا	التطبيق
أسماء الأشخاص المسؤولين عن الحدث	1 – الجاني (حامل البطاقة التي تحمل رقم حساب بأعداد تبدأ من اليسار 453978116759451، وهو مطبوع باللغة الإنجليزية على مساحة التوقيع)
الموضوع الذي شاركت فيه	استعمال المتهم محرراً إلكترونياً مزوراً (كارت فيزا) لسداد ثمن جهاز تليفزيون بمبلغ 4500 جنيه من المحل الذي يعمل المجني عليه مسئولاً للبيع به، وهو محل "----- للأجهزة المنزلية" الكائن 41 ش مكرم عبيد – مدينة نصر أول
الر ابطة الأرشيفية	رقم الكارت المزور (9451) المطبوع على الفيزا رقم الكارت الأصلي (8665) المطبوع على إشعار الخصم
الشكل الوثائقي	بطاقة بلاستيكية مصنوعة من مادة خاصة مستطيلة الشكل يظهر على أحد وجهها الأمامي بيانات رقمية تظهر بأحرف بارزة، تحدد الجهة المصدرة لها، وهوية الشخص حاملها، ونطاق صلاحيتها، واسم الشركة العالمية للبطاقة وشعارها. وعلى الوجه الخلفي يوجد شريط البيانات الممغنط، مخزن عليه جميع البيانات المشفرة الخاصة بحاملها والخاصة بالبنك المصدر لها
التوقيع الإلكتروني	يوجد توقيع إلكتروني مشفر على ظهر البطاقة، كما يوجد رمز الأمان الخاص بالبطاقة

2- سياق الإجراءات[98]

يشمل السياق الإجرائي وفقاً للدبلوماتيك الرقمي إجراءات العمل التي يتم من خلالها إنشاء الوثيقة (الدليل الجنائي)[99]. أما بالنسبة للإثبات الجنائي فالمقصود بسياق الإجراءات هو إجراءات الحصول على الدليل الجنائي الرقمي.

---

[98] قضية جنحة رقم 2569 لسنة 2009 جنح اقتصادية القاهرة.

[99] INTER PARES 3 Project . Diplomatic Analysis template. Retrieved from: http://interpares.org/ip3/display_file.cfm?doc=ip3_template_for_diplomatic_analysis.pdf (last visited 11 / 6 / 2021).

ويمكن تقسيم التحليل الدبلوماتي للمراحل الإجرائية في إنشاء أو استخلاص الدليل الجنائي الرقمي على النحو التالي:

أ) المبادرة أو المرحلة التمهيدية (الإعداد لعملية التحقيق الجنائي): المرحلة التمهيدية لأي إجراء تتكون من تلك الأفعال الخطية أو الشفوية التي تبدأ آلية الإجراء[100]. تبدأ مرحلة المبادرة وفقاً للإثبات الجنائي بقيام المُبلغ بضبط المتهم عند محاولته شراء جهاز تليفزيون بمبلغ 4500 جنيه من المحل الذي يعمل المجني عليه مسئولاً للبيع به، وهو محل "---------- للأجهزة المنزلية" الكائن 41 ش مكرم عبيد – مدينة نصر أول، مستخدماً كارت فيزا لسداد الثمن فقام بسحبه على ماكينة السحب فتبين له تزوير تلك الفيزا لوجود اختلاف في رقم كارت الفيزا المُقدم من المتهم عن الرقم الظاهر في الإيصال الذي خرج من الماكينة. فقام بالتأكد من ذلك من خلال مراجعة البنك، وبناءً عليه قام بالإمساك بالمتهم عند محاولته الهرب وقام بالاتصال هاتفياً بالإدارة العامة لمباحث الأموال العامة للإبلاغ[101].

ب) التحقيق (جمع الوثائق (الأدلة) الرقمية الصحيحة): وفقاً للدبلوماتيك الرقمي تتكون هذه المرحلة الأولية من خلال جمع العناصر اللازمة لتقييم الوضع[102]. تبدأ مرحلة التحقيق وفقاً للإثبات الجنائي، بإجراء التحريات وجمع الوثائق (الأدلة) اللازمة للتحقيق، بعد ضبط الفيزا المستخدمة في الواقعة، والمنسوبة إلى بنك "نات ويست" وتحمل رقم 453978116759451. تبين أن المتهم نيجيري الجنسية وبتفتيش المتهم وقائياً عُثر بحوزته على بطاقة أخرى للبنك الأهلي سوستيه جنرال، كما عُثر في مسكنه على جهاز لاب توب وحقيبة وُجد في داخلها بطاقة منسوبة إلى وزارة التعليم العالي وأُخرى منسوبة إلى "أوشن بنك"، وبناءً عليه تم اصطحاب المتهم لقسم الشرطة.

وبمناقشة المتهم أقرا بحيازته للبطاقات الائتمانية المزورة واستخدام المتهم لإحداها في عملية الشراء من المحل المُشار إليه بعد أن حصل عليهم من أحد أصدقائه.

---

[100] INTER PARES 3 Project . Diplomatic Analysis template, p 1-5.

[101] حسناء على على عبد الغني . (2022). علم الوثائق (الدبلوماتيك) وعلاقته بعلم الإثبات الجنائي الرقمي، الملحق الثاني (وثائق قضية جنحة رقم 2569 لسنة 2009 جنح اقتصادية القاهرة)، ص321 - 329.

[102] INTER PARES 3 Project . Diplomatic Analysis template, p 1-5.

وبسؤال المُبلغ بالمحضر قرر بذات الأقوال السابقة، وقدم صورتي إشعار خصم بمبلغ 4500 جنيه بموجب الكارت رقم 4640166004028665. وتم عرض الكروت الثلاثة المضبوطة على وحدة الفحص المعملي بالإدارة[103].

ج) التشـــاور(فحص المواد الرقمية): تتآلف هذه المرحلة وفقاً للدبلوماتيك الرقمي من جمع الآراء والمشـورة بعد كل البيانات ذات الصـلة والتي تم جمعها[104]. تتضـمن مرحلة التشـاور وفقاً للإثبات الجنائي، إعداد المواد التي تم جمعها للفحص، وقد قامت إدارة مكافحة جرائم التزييف والتزوير (وحـدة البحوث الفنيـة) بفحص الكروت الثلاثـة وتبين تزوير الكـارت المسـتخدم في الشـراء كما ذُكر سـابقاً، والكارت المنسـوب إلى "أوشـن بنك" وسـلامة الكارت المنسـوب للبنك الأهلي سـوسـتيه جنرال، وأرفق تقرير فني بذلك بالمحضـر. كما قامت الإدارة بفحص محتويات الملفات المخزنة على القرص الصـلب لجهاز اللاب توب المضـبوط بحوزة المتهم، وتبين وجود ملف بـداخلـه قـائمـة تحتوي على آلاف من عنـاوين البريـد الإلكتروني لمســتخدمي شــبكة الإنترنت. وقد أفادت الإدارة بأنه تم التزوير عن طريق عملية النســخ الإلكتروني[105]، وذلك باستخدام أجهزة تزوير خاصة يتم تركيبها على أجهزة الصراف الآلي.

---

[103] حسناء على على عبد الغني . (2022). علم الوثائق (الدبلوماتيك) وعلاقته بعلم الإثبات الجنائي الرقمي، الملحق الثاني (وثائق قضية جنحة رقم 2569 لسنة 2009 جنح اقتصادية القاهرة)، ص321 - 329.

[104] INTER PARES 3 Project . Diplomatic Analysis template, p 1-5.

[105] تتم عملية النسخ عن طريق وضع شريط تسجيل إلكتروني على البطاقة الأصلية، وعن طريق تمرير التيار الحراري تحصل عملية نسخ البيانات من البطاقة الأصلية إلى الشريط الممغنط، ثم يتم وضع الشريط الممغنط الذي تم نسخ البيانات عليه على الشريط الفارغ عن طريق التيار الحراري، لكي يتم نسخ جميع البيانات إلى الشريط الفارغ. وغالباً ما تأخذ أجهزة التزوير شكل قارئ بطاقات إضافي يتم وضعه فوق القارئ الأصلي ويعمل على تسجيل كافة البيانات التي يتم مرورها خلاله. **انظر:** ممدوح بن رشيد الرشيد العنزي. (2015). نفس المرجع، ص58،62. ويمكن أن ترفق أجهزة التزوير هذه بلوحة مفاتيح مزورة فوق اللوحة الحقيقية, أو أن ترفق بكاميرا فيديو صغيرة لتصوير الرقم السري الذي يتم إدخاله لكل بطاقة. كما يمكن أن تحتوي الإصدارات الأحدث من أجهزة التزوير هذه على وحدة خاصة تعمل بنظام GSM لإرسال النسخ المشفرة للمحتال. وبمجرد حصول المجرمين على المعلومات ورقم البطاقة سيكون بإمكانهم إنشاء نسخة مزورة مطابقة للبطاقة الائتمانية الأصلية. **انظر:** ثناء أحمد محمد المغربي.(2003).نفس المرجع، ص1140.

د) التداول (مرحلة تدوين النتائج وإعداد التقرير): تتكون هذه المرحلة من اتخاذ القرار النهائي[106]. وفقاً للإثبات الجنائي، تتضمن هذه المرحلة إعداد التقارير عن الأنشطة والفحوص التي تمت، وتدوين النتائج. وتتمثل هذه المرحلة في إعداد محاضر التحريات والضبط والتفتيش وتقرير الفحص الفني وتقديمها للنيابة العامة.

هـ) مراقبة التداول (تقديم حزمة الأدلة): تتكون هذه المرحلة وفقا للدبلوماتيك من الرقابة التي يمارسها شخص طبيعي أو اعتباري غير صاحب الوثيقة الذي يُجسد المعاملة[107].

وفقاً للإثبات الجنائي، تتضمن هذه المرحلة تقديم كل الوثائق والتقارير إلى الفريق القانوني لإرفاقها مع المواد التي سوف يتم تقديمها إلى المحكمة.

و) التنفيذ (إدارة مواد القضية): تتمثل هذه المرحلة وفقاً للدبلوماتيك الرقمي في جميع الإجراءات التي تُضفي الطابع الرسمي على الإجراء. والوثائق التي يتم إنشاؤها في هذه المرحلة هي الوثائق الأصلية التي تُعبر عن الحدث، بمعنى آخر، تؤدي مرحلة التنفيذ إلى إصدار أول وثيقة قادرة على تحقيق النتائج التي قصدها منشؤها[108].

تُشير هذه المرحلة وفقاً للإثبات الجنائي إلى التأكد من توافر الركن المادي والمعنوي لارتكاب الجريمة، يتمثل الركن المادي في اقتراف المتهم لفعل استعمال التوقيع أو الوسيط أو المحرر الإلكتروني المزور. وقد اطمئنت المحكمة لتوافر هذا الركن، نظراً لأنه تم ضبط المتهم حال استعماله الكارت المزور. ويتمثل الركن المعنوي في أن يكون المتهم على علم يقيني بوجود هذا التزوير وفقاً لأحكام المادة (23) من قانون التوقيع الإلكتروني المصري، وهو ما اطمئنت إليه المحكمة أيضاً نظراً لما جاء بالمحضر من محاولة المتهم الهرب حال اكتشاف المجني عليه للواقعة. والوثائق التي يتم إنشاؤها في هذه المرحلة هي وثيقة النطق بالحكم ضد المتهم[109].

يتضح مما سبق، أنه لكي تظهر وثيقة النطق بالحكم في صورتها النهائية فقد مرت بست مراحل إجرائية. هذه المراحل توضح النظم الإدارية والإجرائية والقانونية التي تقوم بها

---

[106] INTER PARES 3 Project . Diplomatic Analysis template, p 1-5.

[107] INTER PARES 3 Project . Diplomatic Analysis template, p 1-5.

[108] INTER PARES 3 Project . Diplomatic Analysis template, p 1-5.

[109] حسناء على على عبد الغني . (2022). علم الوثائق (الدبلوماتيك) وعلاقته بعلم الإثبات الجنائي الرقمي، الملحق الثاني (وثائق قضية جنحة رقم 2569 لسنة 2009جنح اقتصادية القاهرة)، ص321 - 329.

المحكمة لإصـــدار الحكم على المتهم، مما يؤكد على صـحة الوثائق المقدمة، كما أن اكتمال إجراءات إنشـــاء الوثائق يبعث على الثقة في هذه الوثائق. بالإضـــافة إلى أن هذه المراحل تعكس الأنشطة الإجرائية الستة التي حددها نموذج الإثبات الجنائي الرقميDRF.

والجدول رقم (3) يوضـح تطابق إجراءات التحليل الدبلوماتي الرقمي مع إجراءات نموذج الإثبات الجنائي الرقميDRF:

المراحل الإجر ائية	إجراءات التحليل الدبلوماتي	إجراءات الإثبات الجنائي الرقميDRF
المرحلة الأولى	المبادرة	الإعداد لعملية التحقيق الجنائي
المرحلة الثانية	التحقيق	جـمـع الـوثـائـق (الأدلـة) الـرقـمـيـة الصحيحة
المرحلة الثالثة	التشاور	فحص المواد الرقمية
المرحلة الرابعة	التداول	مرحلة تدوين النتائج وإعداد التقرير
المرحلة الخامسة	مراقبة التداول	تقديم حزمة الأدلة
المرحلة السادسة	التنفيذ	إدارة مواد القضية

3 - السياق القانوني: هو النظام القانوني والتنظيمي الذي يتم فيه إنشاء الوثيقة[110]، ويُقصد به هنا الســـياق القانوني للدعوى الجنائية. يظهر الســـياق القانوني في الحكم الصـــادر من المحكمة ضـد المتهم، والذي ينص على: حبس المتهم الأول سـتة أشـهر وكفالة قدرها خمسـمائة جنيه وألزمته المصاريف[111].

وفقاً للحكم الصـــادر فقد تمت معاقبة المتهم وفقاً لأحكام المادة 1/336 من قانون العقوبات، حيث نصت المادة على أنه: "يعاقب بالحبس كل من توصل إلى الإستيلاء على نقود أو عروض أو ســـندات مخالصـــة أو أي متاع منقول وكان ذلك بالاحتيال لســـلب كل ثروة الغير أو بعضها إما باستعمال طرق احتيالية من شأنها إيهام الناس بوجود مشروع كاذب أو واقعة مزورة أو إحداث الأمل بحصـــول ربح وهمي أو تســـديد المبلغ الذي أخذ بطريق الاحتيال أو ايهامهم

---

[110] INTER PARES 3 Project . Diplomatic Analysis template, p 1-5.

[111] انظر الملحق الثاني من رسالة حسناء على على عبد الغني. (2022)، (وثائق قضية جنحة رقم 2569 لسنة 2009جنح اقتصادية القاهرة)، ص321 - 329.

بوجود سند دين غير صحيح أو سند مخالصة مزور إما بالتصرف في مال ثابت أو منقول ليس ملكاً له ولا له حق التصرف فيه وإما باتخاذ اسم كاذب أو صفة غير صحيحة، أما من شرع في النصب ولم يتممه فيعاقب بالحبس مدة لا تتجاوز سنة"[112]. كما نصت المادة 215 من ذات القانون على أنه " كل شخص إرتكب تزويراً في محررات أحد الناس بواسطة إحدى الطرق السابق بيانها يعاقب بالحبس مع الشغل"[113]. كما تمت معاقبة المتهم وفقاً لأحكام المادة 23/ (ج) من قانون تنظيم التوقيع الإلكتروني المصري رقم 15 لسنة 2004، والتي تنص على أنه: "مع عدم الإخلال بأية عقوبة أشد منصوص عليها في قانون العقوبات أو في أي قانون آخر، يُعاقب بالحبس وبغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز مائة ألف جنيه أو بإحدى هاتين العقوبتين كل من: استعمل توقيعاً أو وسيطاً أو محرراً إلكترونياً أو زور شيئاً من ذلك بطريق الإصطناع أو التعديل أو التحوير أو بأي طريق آخر[114].

الوسيط : شريط البيانات الممغنط، يحتوى الشريط الممغنط أو الرقاقة الممغنطة للبطاقة على معلومات تشمل اسم حامل البطاقة ورقم الحساب وتاريخ انتهاء صلاحية البطاقة وكود أو رمز التحقق من البطاقة، حيث يقوم قارئ البطاقة بفك شفرة هذه المعلومات وإرسالها إلى معالج الدفع ثم يتحقق معالج الدفع من توفر الأموال الكافية لإتمام المعاملة ويكمل التاجر عملية البيع[115].

والجدول رقم (4) يوضح مدى مطابقة الفحص الجنائي الرقمي لمنهج علم الدبلوماتيك الرقمي في جريمة استعمال بطاقة الائتمان أو الفيزا المزورة:

---

[112] قانون العقوبات المصري رقم 58 لسنة 1937، المادة 1/336. متاح على الرابط التالي:
https://sites.google.com/site/lawyermohabghaly/project-definition/1-2/qwanyn1937 (last visited 1/2/2020).

[113] قانون العقوبات المصري رقم 58 لسنة 1937، المادة (215) .

[114] قانون التوقيع الإلكترونى المصرى رقم 15 لسنة 2004، المادة 23/ج .

[115] ممدوح بن رشيد الرشيد العنزي. (2015). الحماية الجنائية لبطاقات الدفع الإلكتروني من التزوير، ص47.

وجه المقارنة	الفحص الجنائي الرقمي	عناصرالنقد (الفحص) الدبلوماتي الرقمي	مطابق	غير مطابق
السياق	مضاهاة رقم بطاقة الفيزا المنسوبة إلى بنك "نات ويست" بالرقم المطبوع على إشعار الخصم الذي خرج من ماكينة السحب	سياق المصدر	مطابق	
	إجراءات الإثبات الجنائي في الحصول على الوثائق (الأدلة) الرقمية	سياق الإجراءات	مطابق	
	تحديد الإطار القانوني الذي تتم فيه الدعوى الجنائية	السياق القانوني	مطابق	
	فحص محتويات الملفات المخزنة على القرص الصلب لجهاز اللاب توب.	السياق التقني	مطابق	
الوسيط	فحص الشريط الممغنط	الوسيط		غير مطابق
الخصائص الخارجية	فحص التوقيع الإلكتروني	الخصائص الخارجية		غير مطابق
الخصائص الداخلية	فحص رقم الحساب المطبوع على الفيزا	المسؤول عن التزوير (الجاني)	مطابق	
	تحديد الإجراء الذي شاركت فيه الفيزا	وصف الحدث (الخصائص الداخلية)	مطابق	

يتضح من الجدول السابق أن الفحص الجنائي اقتصر على فحص محتويات الملفات المخزنة على القرص الصلب لجهاز اللاب توب الخاص بالجاني، ومضاهاة رقم بطاقة الفيزا المنسوبة إلى بنك "نات ويست" بالرقم المطبوع على إشعار الخصم الذي خرج من ماكينة السحب، غير أنه وفقاً للدبلوماتيك الرقمي كان يجب فحص الخصائص الخارجية للبطاقة من

حيث شـــريط البيانات الممغنط، والمخزن عليه جميع البيانات المشـــفرة الخاصـــة بحاملها والخاصة بالبنك المصدر لها، بالإضافة إلى فحص التوقيع الإلكتروني المشفر على ظهر البطاقة ورمز الأمان الخاص بالبطاقة حتى يمكن تقييم أصـــالتها وتحديد هويتها. ومن هنا يمكن القول أن الإثبات الجنائي بحاجه إلى علم الدبلوماتيك لتحليل أكثر تفصـــيلاً، حيث يشـــتمل النقد (الفحص) الدبلوماتي على الشكل والمحتوى والسياق.

الجريمة الثانية: اختراق البريد الإلكتروني لشركة أوركتك[116]

المقصـود باختراق البريد الإلكتروني[117] (الدخول غير المشـروع إلى المعلومات والبيانات المرسـلة عن طريق البريـد الإلكتروني). ويعتمـد الاختراق على الســـيطرة عن بُعـد، وهى لا تتم إلا بوجود عاملين:

العامل الأول: البرنامج المسيطر ويعرف "بالعميل Client".

العامل الثانى: الخادم Server الذي يقوم بتسهيل عملية الاختراق[118].

وتتمثل وقائع هذه القضية في قيام مجهول باختراق موقع التحكم في حسـابات البريد الإلكتروني Email Accounts الخاص بالمالك والعاملين بشـركة أوركتك مسـتخدماً بطريقة غير مشـروعة كلمة المرور التي تحصـل عليها كونه أحد العاملين بالشـركة المذكورة سـابقاً وعليه فقد أعـاق (غيَر) الوســـيط الإلكتروني بـأن قـام بمحو البيـانـات الخـاصـــة بـه وجعلـه غير صـــالح للاستعمال بواسطة مالكه.

---

[116] وثائق قضية جنحة رقم 113 لسنة 2019 جنح اقتصادية القاهرة.

[117] عرَف قاموس (ODLIS) البريد الإلكتروني بأنه: بروتوكول إنترنت يسمح لمستخدمي الحاسب الآلي بتبادل الرسائل وملفات البيانات في الوقت الحقيقي "Real Time" (أي في نفس وقت إرسال الرسالة) مع المستخدمين الآخرين، محلياً وعبر الشبكات. ويتطلب البريد الإلكتروني استخدام نظام أو برنامج للرسائل (Message System) يسمح للمستخدم بتخزين وتوجيه الرسائل، وأيضاً استخدام برنامج بريد إلكتروني مع واجهة لإرسال واستقبال الرسائل. ويمكن للمستخدم إرسال الرسائل إلى مستلم واحد له عنوان بريد إلكتروني Email Address معين أو التراسل إلى قائمة توزيع أو قائمة بريدية (Mailing List) دون عمل نسخة ورقية إلا عندما يطلب عمل نسخة مطبوعة. انظر: عائشة أحمد حلمي عبدالعزيز. (2018). نظم إدارة وأرشفة البريد الإلكتروني في المؤسسات الخاصة: دراسة تطبيقية."أطروحة ماجستير"، جامعة الأزهر، ص 16.

[118] عائشة أحمد حلمي عبدالعزيز. (2018). مرجع سابق، ص 198.

النقد الدبلوماتي الرقمي للبريد الإلكتروني كوثيقة إلكترونية ثابتة

- السياق

(1) سـياق المصـدر: تبدأ عملية الإثبات الجنائي والنقد الدبلوماتي بفحص مصـدر الوثيقة، وذلك بالبحث عن من هو الشـخص المسـؤول عن اختراق موقع التحكم في حسـابات البريد الإلكتروني، ثم التعرف على المصدر وتحديده من خلال مخاطبة الموقع المستضيف للإيميلات الخاصـة بالشـركة، حيث أنه بعد ملاحظة اختراق موقع التحكم في حسـابات البريد الإلكتروني Email Accounts المسـتضـافة في موقع (Siteground.com@)، قامت شـركة أوركتك بتغيير كلمة المرور السـرية على الفور من جانب الشـركة، ثم مخاطبة الموقع المسـتضـيف للإيميلات الخاصـة بهم(Siteground.com@)، والذي أفاد بأن من قام بالإختراق هو مسـتخدم الرقم التعريفي156.222.198.82 IP [119].

وبناءً عليه قامت إدارة مكافحة جرائم الحاسـبات وشـبكات المعلومات (قسـم المسـاعدات الفنية) بتتبع الرقم التعريفي 156.222.198.82 IP المشـار إليه من على شـبكة المعلومات الدولية (الإنترنت)، والذي تبين أنه صادر من جهاز حاسب آلي مرتبط بجهاز ADSL ماركة TE DATA أبيض اللون، ، كما ثبت أن هذا الجهاز متصـل بخط تليفون أرضـي (----) مسجل بالشركة المصرية للاتصالات باسم المتهم (-----)، وعنوانه (------)[120].

ويعتبر ما قامت به إدارة مكافحة جرائم الحاسـبات وشـبكات المعلومات مطابقاً لمنهج الدبلوماتيك الرقمي، حيث أنه للتحقق من مدلول الوثيقة يجب على الوثائقي إثبات نسـبة الوثيقة إلى منشـأها، وذلك بفحص الوثيقة ومحاولة إيجاد ما يربطها بذلك المصـدر (الجاني) وهو ما قامت به بالفعل إدارة مكافحة جرائم الحاسـبات من خلال فحص سـجلات الدخول للبريد الإلكتروني وتحديد عنوان IP وتتبع مصـدره. بالإضـافة إلى أنه لتحديد هوية الوثيقة الرقمية (البريد الإلكتروني) وتقييم صـحتها وفقاً للدبلوماتيك الرقمي يجب تحديد عناصـر

---

[119] انظر الملحق الثالث من رسالة حسناء على على عبد الغني. (2022)، (صوره ضوئية لوثيقة البريد الإلكتروني لقضية جنحة رقم 113 لسنة 2019 جنح اقتصادية القاهرة)، ص330 – 332.

[120] انظر الملحق الرابع من رسالة حسناء على على عبد الغني. (2022)، (تقرير الفحص الفني لقضية جنحة رقم 113 لسنة 2019 جنح اقتصادية القاهرة)، ص333 – 335.

الشـكل الخـارجي والـداخلي المطلوبـة للنقـد الـدبلوماتي من خلال ميتـاداتا الهويـة والتكامل الموجودين بالمرحلة الفكرية والمنطقية لوثيقة البريد الإلكتروني.

والجدول رقم (5) يوضح ميتاداتا الهوية لوثيقة البريد الإلكتروني الذي تم اختر اقه:

أ - ميتاداتا الهوية

عناصر الميتاداتا	التطبيق
أسـماء الأشـخاص المسؤولين عن الحدث	1 – صاحب الرقم التعريفي 156.222.198.82 IP (المخترق) 2 – المجني عليهم (العاملين بشركة أوركتك للبرمجيات)
التـاريخ ووقـت الإنشـاء (الإخـتـراق وحـذف الإيميلات)	7 سبتمبر 2018 – الساعة 12:47بتوقيت جرينتش
الموضـوع الذي شـاركت فيه	التلاعب في حسابات البريد الإلكتروني الخاص بالعاملين بشركة أوركتك للبرمجيات، وذلك بحذف هذه الإيميلات
الرابطة الأرشيفية	تسجيلة الدخول للموقع من خلال سجل المراجعة
الشكل الوثائقي	البريد الإلكتروني عبارة عن رسـائل مرسـلة ومسـتلمة من أجهزة الحاسـب الآلي عن طريق شـبكة الإنترنت، ويسـمح نظام البريد الإلكتروني لمسـتخدمي الحاسـب الآلى على الشـبكة بإرسـال النـص، الرسـومات، الفيـديو وأنـواع أخرى من الملفـات للمسـتخدمين الآخرين. وعادة ما يكون لدى مسـتخدمي شـبكة الإنترنت صندوق بريد إلكتروني يتلقى، يخزن، ويدير مراسلاتهم، ويمكن للمتلقي أن يختار عرض، طباعة، حفظ، تعديل، والرد على الرسالة، أو إعادة توجيهها كما يسمح نظام البريد الإلكتروني للمستخدمين بالحذف أو الإضافة
التوقيع الإلكتروني	لا يوجـد توقيع إلكتروني وإنمـا توجـد كلمـة مرور لعنوان البريـد الإلكتروني وهو ما يُسمى بتوقيع البريد الإلكتروني

ب - ميتاداتا التكامل

جدول رقم (6) يوضح ميتاداتا التكامل لوثيقة البريد الإلكتروني الذي تم اختراقه

عناصر الميتاداتا	التطبيق
أسماء الأشخاص المسؤولين عن الحدث	1 – صـــاحـب الرقم التعريفي IP 156.222.198.82 (المخترق) 2 – المجني عليهم (العاملين بشركة أوركتك للبرمجيات)
الشخص أو المكتب المسؤول عن حـفـظ الـوثـيـقـة (الإيـمـيـلات الخاصة بالشركة)	الموقع المستضيف للإيميلات الخاصة بالشركة وهو (@Siteground.com)
التغيرات التقنية	حدث تغييرات في المكونات الرقمية لوثيقة البريد الإلكتروني بسبب حذف الإيميلات الخاصة بالشركة
مؤشـــر وجود أو إزالـة التوقيع الإلكتروني	قيام الجاني باختراق البريد الإلكتروني باستخدام كلمة المرور التي تحصـل عليها كونه أحد العاملين بالشـركة بطريقة غير مشـروعة وبعد ملاحظة اختراق موقع التحكم في حسـابات البريد الإلكتروني قامت شـركة أوركتك بتغيير كلمة المرور السرية على الفور
المكتب المسؤول بصفة أساسية عن الوثيقة (الإيميلات الخاصة بالشركة)	شركة أوركتك للبرمجيات
التاريخ ووقت الإزالة من النظام (الإختراق وحذف الإيميلات)	7 سبتمبر 2018 – الساعة 12:47بتوقيت جرينتش

يتضح مما سبق، أنه من خلال تحليل عناصر الميتاداتا والتي تعبر عن الخصائص الداخلية والخارجية يمكن تحديد اسم الجاني والمجني عليه وتاريخ الاختراق من خلال تتبع عنوان IP والموضوع الذي شاركت فيه، كذلك يمكن الكشف عن التغييرات التي حدثت في حسابات البريد الإلكتروني من خلال ميتاداتا التكامل.

(2) سياق الإجراءات[121]

يمكن تقسيم التحليل الدبلوماتي للمراحل الإجرائية في إنشاء أو استخلاص الدليل الجنائي الرقمي على النحو التالي:

أ) المبادرة أو المرحلة التمهيدية (الإعداد لعملية التحقيق الجنائي):

تبدأ مرحلة المبادرة وفقاً للإثبات الجنائي، بقيام مدير وشريك شركة أوركتك بمخاطبة الموقع المستضيف للإيميلات الخاصة بالشركة (@Siteground.com)، لمعرفة عنوان IP الذي يمكنه الوصول إلى البريد الإلكتروني، ثم الإبلاغ عن قيام مجهول باختراق موقع التحكم في حسابات البريد الإلكتروني Email Accounts الخاص بالشركة والمستضافة في موقع (@Siteground.com).

شكل رقم (6) يوضح شعار الشركة المستضيفة للإيميلات وهي شركة Siteground

ب) التحقيق (جمع الوثائق (الأدلة) الرقمية الصحيحة):

تبدأ مرحلة التحقيق وفقاً للإثبات الجنائي بإجراء التحريات وجمع الوثائق (الأدلة) اللازمة للتحقيق، بعد معرفة الحاسب الذي تم الاتصال منه (الجهاز الذي حدثت العملية من خلاله) وتحديد موقعه الجغرافي، ثبت أن هذا الجهاز متصل بخط تليفون أرضي (-------) مسجل بالشركة المصرية للاتصالات باسم المتهم وعنوانه، وقد أيد ذلك وشهد به كل من النقيب/ أحمد شريف – (الضابط بقسم المباحث الجنائية)، والرائد/ حسام يُسري - (الضابط بقسم المساعدات الفنية بالإدارة) – بتحقيقات النيابة العامة.

وبناءً عليه تم الوصول إلى المتهم وقد أثبتت التحريات أن المُتهم سبق له العمل بالشركة المشار إليها مده لم تتجاوز الثلاث أسابيع وأنه تم رفده من الشركة على إثر مشادة كلاميه بينه وبين أحد العاملين بالشركة دون السماح له بتوضيح موقفه من المشاده، الأمر الذي أصاب حفيظته وقرر على إثر ذلك الانتقام من الشركة بالفعل الذي اقترفه.

---

[121] قضية جنحة رقم 113 لسنة 2019 جنح اقتصادية القاهرة.

وبســـؤال المتهم عن كيفية ارتكابه للواقعة: أفاد المتهم أنه أثناء فترة عمله بالشـــركة ولطبيعة عمله بها ضـــمن فريق تكنولوجيا المعلومات (IT) كان له صـــلاحية الولوج على الخادم الخاص بالشـــركة بواســـطة كلمة مرور ســـرية كان يعلمها بحكم طبيعة عمله واســـتخدمها في ارتكاب الواقعة.

كما تم ضـــبط وتفتيش شـــخص ومســـكن وملحقات مســـكن المتحرى عنه (المتهم)، لضبط ما يحوزه أو يحرزه من ثمة أجهزة حاسب آلي ثابتة أو محمولة أو آية أدوات أخرى. وعليه فقد تم تحريز كل من وحدة المعالجة المركزية المرتكب بواســـطتها الواقعة محل الاتهام، وجهاز تجميع وصلات الإنترنت.

كما تتضمن هذه المرحلة التحقق من إجراءات حفظ وتحريز الأدلة، والتي تتمثل فيما يلي:

- تحريز محضـــر الضـــبط وإذن النيابة العامة وتقرير الفحص الفني داخل مظروف أبيض اللون مجمع عليه بالجمع الأبيض في عدة مواضع بخاتم تقرأ بصمته أحمد شريف ضابط شرطة تمت.
- تحريز وحدة المعالجة المركزية المرتكب بواســـطتها الواقعة ولفها بلاصـــق ووضـــع كارت معلومات (ورقة بيضـــاء اللون) مجمع عليها بالجمع الأبيض في عدد واحد موضـــع بخاتم تقرأ بصمته أحمد شريف ضابط شرطة تمت.
- كما تم تحريزجهاز ADSL المستخدم في الاتصال بشبكة الإنترنت ولفه بالدوبار ووضع كارت معلومات مجمع عليه بالجمع الأبيض في عدد واحد موضع بخاتم تقرأ بصمته أحمد شريف ضابط شرطة تمت.
- كذلك تم تحريزجهاز تجميع وصـــلات الإنترنت بوضـــع كارت معلومات (ورقة بيضـــاء اللون) مثبت بها مواصـــفات الحرز ومجمع عليه بالجمع الأبيض في عدد واحد موضـــع بخاتم تقرأ بصمته أحمد شريف ضابط شرطة تمت[122].

[122] انظر الملحق الخامس من رسالة حسناء على على عبد الغني. (2022)، (محضر التحريات ومحضر الضبط والتفتيش لقضية جنحة رقم 113 لسنة 2019 جنح اقتصادية القاهرة)، ص 336 – 340.

ج) التشاور(فحص المواد الرقمية):

بعد التحقق من فحص إجراءات حفظ وتحريز الأدلة يتم فحص المحتوى من خلال مراجعة سجلات الوصول إلى لوحة التحكم، والتي تشتمل على عنوانIP الخاص بالمتسلل، وتاريخ ووقت حدوث الإختراق باليوم والساعة. وقد أثبت الفحص حذف حسابات البريد الإلكتروني الخاصة بالعاملين بالشركة . وعلى الرغم من أن دلائل الصحة في الإثبات الجنائي الرقمي تركز على محتوى الوثيقة بدلاً من جوانبها الشكلية مثل الدبلوماتيك الرقمي إلا أن حماية العرض الوثائقي والرقمي تعتبر مسألة ضمنية في ممارسات الإثبات الجنائي الرقمي. لذلك فإن أي تغيير أو حذف لحسابات البريد الإلكتروني يؤثر على العرض الوثائقي لشكل البريد الإلكتروني. ويعتبر ما قامت به إدارة مكافحة جرائم الحاسبات وشبكات المعلومات مطابقاً لمنهج الدبلوماتيك الرقمي، إلا أنه وفقاً للدبلوماتيك الرقمي كان يجب فحص التناقضات في نظام تشغيل البريد الإلكتروني من خلال فحص التغيرات في نظام الملفات، للتأكد من أن المحتوى المُحمل سابقاً لازال موجوداً أو لا، واستقصاء أنشطة البريد الإلكتروني من خلال أدلة التطبيقات.

د) التداول (مرحلة تدوين النتائج وإعداد التقرير):

تتمثل هذه المرحلة في إعداد محاضر التحريات والضبط والتفتيش وتقرير الفحص الفني وتقديمها للنيابة العامة.

هـ) مر اقبة التداول (تقديم حزمة الأدلة):

تتضمن هذه المرحلة تقديم كل الوثائق والتقارير إلى الفريق القانوني لإرفاقها مع المواد التي سوف يتم تقديمها إلى المحكمة.

و) التنفيذ (إدارة مواد القضية):

تُشير هذه المرحلة إلى التأكد من توافر الركن المادي والمعنوي لارتكاب الجريمة، يتمثل الركن المادي في اقتراف المتهم لأي فعل من الأفعال التي تُشكل النشاط الإجرامي محل الركن المادي للجرائم المنصوص عليها في قانون الاتصالات، ويتمثل الركن المعنوي للجريمة في أن يكون المتهم عالماً بمباشرة النشاط الإجرامي محل الركن المادي وأن تتجه إرادته إلى تحقيق ذلك، وفقاً لأحكام المادة (23) من قانون التوقيع الإلكتروني المصري.

وكانت المحكمة قد اطمئنت إلى أن المتهم تعمد إزعاج ومضايقة الغير بإساءة استعمال أجهزة الاتصالات، وذلك باختراقه ودخوله عمداً على الوسيط الإلكتروني (البريد الإلكتروني) الخاص بالمالك والعاملين بشركة أوركتك مستخدماً بطريقة غير مشروعة كلمة المرور التي تحصل عليه كونه أحد العاملين بالشركة المذكورة سابقاً وعليه فقد عيب الوسيط الإلكتروني بأن قام بمحو البيانات الخاصة به وجعله غير صالح للاستعمال بواسطة مالكه، وذلك أخذاً بإقرار المتهم بارتكابه الجرائم المسندة إليه استدلالاً وتحقيقاً والذي أكدها ما ثبت بتقرير الفحص الفني، وعليه فقد استخلصت المحكمة أن المتهم اتجهت إرادته الآثمة عن طواعية وحرية اختيار إلى اقتراف الاتهامات المسندة إليه مما يثبت معه توافر أركان الجرائم في حقه بركنيها المادي والمعنوي. كما تتضمن مرحلة التنفيذ وثيقة النطق بالحكم ضد المتهم.

3 - السياق القانوني:

يظهر السياق القانوني في الحكم الصادر من المحكمة ضد المتهم، ووفقاً للحكم الصادر فقد تمت معاقبة المتهم وفقاً لأحكام المواد (14)، (18)، (38) من قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018، وعملاً بنص المادة (313) من قانون الإجراءات الجنائية، المادة 23/ (ب)، 23/ (هـ) من قانون تنظيم التوقيع الإلكتروني المصري رقم 15 لسنة 2004[123].

والجدول رقم (7) يوضح مدى مطابقة السياق القانوني للأحكام القضائية الصادرة بشأن هذه الدعوى الجنائية (اختراق البريد الإلكتروني للعاملين بشركة أوركتك).

الإتهام	السياق القانوني للدعوى الجنائية	الحكم
اختراق الوسيط الإلكتروني (البريد الإلكتروني) الخاص بالمالك	تنص المادة (14) من قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018 على أنه: "يُعاقب بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من دخل عمداً، أو دخل بخطأ غير عمدي وبقي بدون وجه حق، على موقع أو حساب خاص أو نظام معلوماتي محظور الدخول عليه.	تغريم المتهم غرامة مالية مائة ألف جنيه عن الاتهام المسند إليه ومصادرة الأجهزة التي

[123] وثائق قضية جنحة رقم 113 لسنة 2019 جنح اقتصادية القاهرة.

الإتهام	السياق القانوني للدعوى الجنائية	الحكم
والعاملين بشركة أوركتك وتعطيله عن أداء وظيفته[124].	- فإذا نتج عن ذلك الدخول إتلاف أو محو أو تغيير أو نسخ أو إعادة نشر للبيانات أو المعلومات الموجودة على ذلك الموقع أو الحساب الخاص أو النظام المعلوماتي، تكون العقوبة الحبس مدة لا تقل عن سنتين، وغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مائتي ألف جنيه أو بإحدى هاتين العقوبتين. وحيث أنَ المادة (18) من ذات القانون تنص على أن "يعاقب بالحبس مدة لا تقل عن شهر، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من أتلف أو عطل أو أبطأ أو اخترق بريداً إلكترونياً أو موقعاً أو حساباً خاصاً بآحاد الناس. فإذا وقعت الجريمة على بريد إلكتروني أو موقع أو حساب خاص بأحد الأشخاص الاعتبارية الخاصة، تكون العقوبة الحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مائتي ألف جنيه أو بإحدى هاتين العقوبتين". كما تنص المادة (38) من ذات القانون على أن "مع عدم الإخلال بحقوق الغير حسن النية، على المحكمة في حالة الحكم بالإدانة في أي جريمة من الجرائم المنصوص عليها في هذا القانون أن تقضي بمصادرة الأدوات والآلات والمعدات والأجهزة مما لا يجوز حيازتها قانوناً، أو غيرها مما يكون قد استخدم في ارتكاب الجريمة، أو سهل أو ساهم في ارتكابها"[125].	استعملت في ارتكاب هذه الجريمة وأمرت المحكمة بايقاف عقوبة الغرامة المقضي بها لمدة ثلاث سنوات تبدأ من صيرورة هذا الحكم نهائياً والزمته المصروفات الجنائية[126].

[124] وثائق قضية جنحة رقم 113 لسنة 2019 جنح اقتصادية القاهرة.

[125] قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لسنة 2018 . تم نشر هذا القانون في الجريدة الرسمية – العدد 32 مكرر (ج) في 14 أغسطس سنة 2018م ، المادة (14)، (18)، (38). متاح على الرابط التالي : https://drive.google.com/file/d/(last visited 11/10/2020).

[126] وثائق قضية جنحة رقم 113 لسنة 2019 جنح اقتصادية القاهرة.

يتضح من الجدول السابق أنه عند مقارنة نصوص القوانين الموجودة بالوثائق بالتهم المبينة بالدعوى الجنائية، تبين أنَ:

- الحكم القانوني الصادر بشأن هذه الدعوى الجنائية يتم وفقاً للقوانين المنصوص عليها في وثائق القضية.
- السياق القانوني المعلن عنه في المحكمة الإقتصادية مطبقاً بالفعل في الوثائق، أي أن الوثائق الواردة في ملف القضية أُنشئت وفقاً للسياق القانوني للمحكمة، وهو ما يُعتبر مطابقاً لمنهج علم الوثائق (الدبلوماتيك)، حيث أنه وفقاً لمنهج علم الدبلوماتيك يجب على الوثائقي (الدبلوماتي) عند فحص السياق القانوني للوثيقة التأكد من أنها أُنشئت وفقاً للسياق القانوني للجهة التي أنشأت الوثائق، أي أن السياق المعلن عنه مطبقاً بالفعل في الوثائق.

4 - السياق التقني[127]:

يُقصد بالسياق التقني هنا البيئة التقنية للنظام الذي أنشأ وثيقة البريد الإلكتروني. وقد قامت إدارة مكافحة جرائم الحاسبات وشبكات المعلومات بفحص مكونات جهاز الحاسب الآلي الذي تم ضبطه ومحتوياته على النحو التالي:

فحص مكونات الجهاز: بفحص مكونات جهاز الحاسب الآلي، تبين أن الجهاز المضبوط عبارة عن وحدة معالجة مركزية (CPU) سوداء اللون تجميع محلي لا تحمل أرقاماً مسلسلة مدون عليها من الخارج باللغة الإنجليزية كلمة AEG . كما تبين أن الجهاز مزود بكارت شبكة للاتصال بشبكة الإنترنت.

فحص محتويات الجهاز: بفحص محتويات وحدة المعالجة المركزية (CPU) تبين وجود آثار ودلائل على استخدام الموقع الخاص بالشركة المعنون Siteground.com@.

ويُعتبر ما قامت به إدارة مكافحة جرائم الحاسبات وشبكات المعلومات مطابقاً لمنهج علم الدبلوماتيك الرقمي، إلا أنه وفقاً لمنهج علم الدبلوماتيك كان يجب تحديد سعة الجهاز أو

[127] انظر الملحق الرابع رسالة حسناء على على عبد الغني. (2022)، (تقرير الفحص الفني لقضية جنحة رقم 113 لسنة 2019 جنح اقتصادية القاهرة)، ص 333 - 335.

مواصفات ذاكرة الجهاز الذي يُستخدم لعرض الوثائق، كما يجب تحديد سرعة وحدة المعالجة المركزية (CPU) .

كذلك يجب تحديد المكونات التقنية لنظام تشغيل البريد الإلكتروني، وبرمجيات النظام، والبرامج التطبيقية، وبرمجيات الشبكة التي يتم تحميلها على جهاز الحاسب الآلي لتدير الشبكة مثل بروتوكولات إرسال واستقبال رسائل البريد الإلكتروني، كما يجب تحديد العلاقات بين الملفات داخل النظام وبيانات عن صيغة الملف مثل معلومات عن إدارة النظام، أكواد موقع التحكم في حسابات الإيميلات الخاصة بالشركة، كل هذه المعلومات ينبغي تحديدها وحفظها لأنها تعطي بيانات أساسية سياقية وبنائية للوثائق، كما أن هذه المعلومات تعبر عن الخصائص الخارجية للبريد الإلكتروني.

- الوسيط

أجهزة شبكة الإنترنت "Network Hardware" وتضم كروت الشبكة، ووصلات الشبكات "Cables"، ومعدات الاتصال بالشبكة "Communication Equipment".

والجدول رقم (8) يوضح مدى مطابقة الفحص الجنائي الرقمي لمنهج علم الدبلوماتيك الرقمي في جريمة اختراق البريد الإلكتروني:

وجه المقارنة	الفحص الجنائي الرقمي	عناصرالنقد (الفحص) الدبلوماتي الرقمي	مطابق	غير مطابق
الخصائص الخارجية	فحص عنوان البريد الإلكتروني وكلمة المرور الخاصة به	الخصائص الخارجية (خصائص العرض)	مطابق	
الخصائص الداخلية	فحص سجل المراجعة	الخصائص الداخلية	مطابق	غير مطابق
	تحديد عنوان IP	المسؤول عن الإختراق	مطابق	
	تحديد تاريخ الإختراق	التاريخ الزماني	مطابق	
	تحديد الموقع الجغرافي للجهاز الذي حدثت العملية من خلاله	التاريخ المكاني	مطابق	

وجه المقارنة	الفحص الجنائي الرقمي	عناصرالنقد (الفحص) الدبلوماتي الرقمي	مطابق	غير مطابق
	تحديد الموضوع الذي شاركت فيه الوثيقة	وصف الحدث	مطابق	
الوسيط	فحص كروت الشبكة، ووصلات الشبكات الخاصة بالإنترنت	الوسيط	مطابق	
السياق	تتبع الرقم التعريفيIP	سياق المصدر	مطابق	
	تحديد إجراءات الإثبات الجنائي	سياق الإجراءات	مطابق	
	تحديد الإطار القانوني الذي تتم فيه الدعوى الجنائية	السياق القانوني	مطابق	
	الفحص الفني لمكونات ومحتويات جهاز الحاسب الآلي	السياق التقني	مطابق	

يوضح الجدول السابق أن استخراج عناصر النقد الدبلوماتي الرقمي تعكس خطوات الفحص الجنائي الرقمي، وتحقق النتائج المرجوة من الفحص، وهو ما يؤكد على دور علم الدبلوماتيك الرقمي في مجال الإثبات الجنائي الرقمي.

الجريمة الثالثة: تزوير مو اقع البريد الإلكتروني[128]

تتمثل وقائع هذه الجريمة في قيام المتهمين بتكوين تشكيل عصابي تخصص في النصب على الشركات الأجنبية عن طريق إرسال رسائل بريد إلكتروني خادعة لضحاياهم، وأن المتهم الأول كان دوره فتح حساب لدى البنك الوطني المصري لتلقي الأموال المرسلة من الشركات الأجنبية التي يتم استهدافها بينما يتولى باقي أفراد التشكيل عمليات القرصنة وتقليد صفحات بعض المواقع وعناوين البريد الإلكتروني وإرسال رسائل خادعة لضحاياهم طالبين تحويل الأموال على حساب شريكهم الأول الذي يقوم بصرفها واقتسامها فيما بينهم. وفيما يلي الاتهامات الموجهة إليهم:

[128] وثائق قضية جنحة رقم 844 لسنة 2013 جنح اقتصادية القاهرة.

- الاستيلاء بطريق الاحتيال على أموال مملوكة للمجني عليهم.
- تزوير محرر الكتروني (البريد الإلكتروني) بطريق الاصطناع لشركة (----) للملابس الجاهزة، وتم استعماله في التهمة الأولى.
- إختراق وسائط إلكترونية لآخرين من ضمنهم المجني عليه .

عناصر النقد:

- السياق

1 - سياق المصدر

تبدأ عملية الإثبات الجنائي والنقد الدبلوماتي بفحص مصدر الوثيقة، وذلك بالبحث عن من هو الشخص المسؤول عن تزوير موقع البريد الإلكتروني لشركة (----) للملابس الجاهزة، ثم التعرف على المصدر وتحديده من خلال فحص عنوان البريد الإلكتروني المزور للمجني عليه (heshamamer@heshamtex.com)، والذي يعمل مدير تصدير لشركة (----) للملابس الجاهزة، ثم فحص الرسالة المرسلة وتحديد مصدرها عن طريق عنوان IP، لأن الرسالة لا تحمل في محتواها معلومات عن المرسل فقط، وإنما يمكن معرفة المكان الذي تم إرسال الرساله منه عن طريق استخدام عنوان IP الذي يرفق مع كل رسالة، وتبعاً لذلك تم تحديد المتهمين.

2 - سياق الإجراءات

يمكن تقسيم التحليل الدبلوماتي للمراحل الإجرائية في إنشاء الدليل الجنائي على النحو التالي:

أ) المبادرة (الإعداد لعملية التحقيق الجنائي):

تبدأ مرحلة المبادرة بمجرد إبلاغ المجني عليه الإدارة العامة لمباحث الأموال العامة بتعرضه لواقعة نصب واحتيال واختراق للبريد الإلكتروني الخاص به على شبكة المعلومات الدولية "الإنترنت" من خلال أحد الأشخاص "الهاكرز".

ب) التحقيق (جمع الوثائق (الأدلة) الرقمية الصحيحة):

تبدأ مرحلة التحقيق وفقاً للإثبات الجنائي بإجراءات جمع الاستدلالات، والتي أثبتت أن المجني عليه تعرف على إحدى العميلات خلال تواجده بدولة ألمانيا، وتُدعى "----" وأنه اتفق

والأخيرة على عقد صـفقات تجارية فيما بينهما وتبادلا عنوان البريد الإلكتروني الخاص بكل منهما، وأنه بالفعل تم التعامل معها بتاريخ 27 إبريل 2013، وذلك بإرسـال صـفقة (بشـاكير بحر) بقيمة إجمالية 6400 يورو. وقد قامت العميلة بإرسـال نصـف المبلغ، وأنه إنتظر إرسـال باقي المبلغ (3200 يورو) عقب ذلك غير أنها لم تقم بإرساله، وبالاستفسار من العميلة تبين أنها أرسلت باقي المبلغ على حساب (شركة تو ام (tow.m) بالبنك الوطني المصري فرع الحجاز)، وأن رقم الحسـاب (-----)، وذلك بناءً على رسـالة بريد إلكتروني من عنوان مشـابه لعنوان الشـاكي طلب فيه إرسال المبلغ على الحساب الآنف بيانه، وقدم الشاكي صورة ضوئية من إشعار مرسل من البنك الخاص بالعميلة. وبسؤال المتهم الأول بمحضر جمع الاستدلالات قرَر أنَ المدعو (---) (المتهم الثالث)أوهمه بكونه مندوب شـركة سـلوفينية وحصـل منه على أجهزة طبية، وتم تحويل مبالغ إلى حسـابه عن طريق هذه الشـركة، وأضـاف أن الجهاز الطبي ثمنه 3200 يورو، وأقرَ بعدد عشـر تحويلات عن طريق النيجيريين (----)، (----)، (-----)، ومنها التحويل الخاص بالعميلة (-----).

وقد تمكن محرر محضر جمع الاستدلالات من ضبط المتهمين النيجيريين بعد إقرارهم بالجرائم،

وقد أكدَت التحريات السـرية عن قيام المتهمين بتكوين تشـكيل عصـابي تخصـص في النصب على الشـركات الأجنبية عن طريق إرسال رسـائل بريد إلكتروني خادعة لضحاياهم وأن المتهم الأول كان دوره فتح حساب لدى البنك الوطني المصري لتلقي الأموال المرسلة من الشركات الأجنبية التي يتم استهدافها بينما يتولى باقي أفراد التشكيل عمليات القرصنة وتقليد صفحات بعض المواقع وعناوين البريد الإلكتروني وإرسـال رسـائل خادعة لضـحاياهم طالبين تحويل الأموال على حساب شريكهم الأول الذي يقوم بصرفها واقتسامها فيما بينهم.

كما تتضـمن هذه المرحلة إجراءات حفظ وتحريز الأدلة، حيث تم ضـبط عدد أربعة أجهزة حاسـب آلي محمول، وعدد ثلاثة وحدات ذاكرة نقالة (فلاش ميموري) وكمية من صـور لرسائل خادعة منسوبة للكثير من البنوك والشركات الأجنبية يستخدمها المتهمون في نشاطهم وعدد أحد عشرة هاتفاً محمولاً ماركات مختلفة.

ج) التشاور(فحص المواد الرقمية):

تتضـمن مرحلة التشـاور وفقاً للإثبات الجنائي إعداد المواد التي تم جمعها للفحص، وبفحص محتوى أجهزة الحاسـب الآلي التي تم ضـبطها ووحدات الذاكرة النقالة والهواتف المحمولة تبين تحميلهم بالكثير من الرسـائل الإلكترونية المتبادلة بين المتهم الأول وباقي المتهمين بشـأن نشـاطهم، والكثير من الرسـائل الإلكترونية الواردة للمتهم الأول تفيد تحويلات بنكية من بنوك أجنبية ومنها رسـائل مرسـلة من باقي المتهمين، ورسـائل احتيالية مرسـلة لمئات الأشـخاص تفيد بوجود مبالغ مالية ضخمة داخل صناديق شحن يستخدمها المتهمون في نشاطهم الإجرامي منسـوبة لهيئة الأمم المتحدة ووزارة العدل الأمريكية، وصـور تحقيق شـخصـية وجوازات سـفر لأشـخاص من جنسـيات أجنبية وعربية معدة للتزوير، والكثير من أسـماء وبيانات شـركات أجنبية يسـتهدفها المتهمون في إرسـال الرسـائل الاحتيالية ومن بينها شـركة الشـاكي. وبفحص عنوان البريد الإلكتروني الخاص بالمتهم الأول تبين أن كلمة المرور الخاصة به Ahmed 112000. وبفحص الرسـائل الواردة تبين وجود رسـالة مسـتلمة من المتهم الثالث (------) وهي عبارة عن استمارة تحويل مبلغ 3200 يورو من بنك NLB في سلوفينيا إلى حساب المتهم الأول (شركة تو ام (tow.m) بالبنك الوطني المصـري فرع الحجاز). وبفحص رسـائل الهواتف المحمولة تبين أنها تحتوي على بيانات بنكية بين الطرفين مرفق بها صورة الاستمارة سالفة الذكر إلى حساب المتهم الأول. كما تحتوي تلك الرسـائل على اتفاق بين الطرفين على مكان التقابل ومعرفة نسـبة الربح والتي قدرها المتهم بـ10% إلى 15 %[129].

وقد أيد ذلك محرر التقرير (المهندس/ باسم ممدوح – الضابط بإدارة مكافحة جرائم التزييف والتزوير) وشهد به بتحقيقات النيابة العامة.

ويعتبر ما قامت به إدارة مكافحة التزوير والتزييف مطابقاً لمنهج علم الدبلوماتيك الرقمي، حيث أنه وفقاً للدبلوماتيك الرقمي لتقييم صـحة وأصـالة الوثائق يجب فحص الخصـائص الخارجية والمتمثلة في فحص عنوان البريد الإلكتروني الخاص بالمتهم الأول وفحص كلمة المرور الخاصـة بعنوان البريد الإلكتروني، وفحص صـيغ الملفات وبرامج القرصـنة التي تم اسـتخدامها حتى يمكن تقييم صـحة وثيقة البريد الإلكتروني، وهو ما قامت به بالفعل إدارة

[129] وثائق قضية جنحة رقم 844 لسنة 2013 جنح اقتصادية القاهرة.

مكافحة التزوير والتزييف، بالإضافة إلى فحص العناصر الداخلية والمتمثلة في فحص محتوى الرسائل الصادرة والواردة، والتي يمكن من خلالها تحديد الجاني وتوقيت الجريمة والحدث الذي شاركت به.

- **العناصر الخارجية لوثائق (أدلة) إثبات تزوير البريد الإلكتروني وفقاً للدبلوماتيك الرقمي:**
- **خصائص العرض**

توجد عدة وثائق (أدلة) رقمية بعضها رسائل بريد إلكتروني والآخر رسائل هاتف محمول، بالنسبة لرسائل البريد الإلكتروني توجد رسالة بريد إلكتروني صادرة ورسالة واردة، الرسالة الصادرة عبارة عن نص مكتوب لا يوجد بها أي تسجيلات صوتية أو صور أو مرفقات. أما الرسالة الواردة فهي عبارة صورة ضوئية لا تحوي أي تسجيلات صوتية أو نص مكتوب.

أما رسائل الهاتف المحمول الواردة والصادرة فهي عبارة عن نص مكتوب مرفق بها صورة استمارة تحويل مبلغ مالي من البنك لا تحوي أي تسجيلات صوتية أو مرفقات أخرى.

- **لا يوجد توقيع إلكتروني** وإنما توجد كلمة مرور لعنوان البريد الإلكتروني وهو ما يُسمى بتوقيع البريد الإلكتروني.
- **كذلك لا توجد علامات خاصة** سواء لرسائل البريد أو رسائل المحمول.

- **العناصر الداخلية**

العناصر الداخلية	رسالة البريد الصادرة	رسالة البريد الواردة
المسئول (المرسل)	(عنوان البريد الإلكتروني المزور لمدير تصدير شركة ------- للملابس الجاهزة) heshamamer@heshamtex.com وهو مكتوب باللغة الإنجليزية في أعلى الرسالة، حيث تبدأ رسائل البريد الإلكتروني باسم المرسل أو البريد الإلكتروني الخاص به إن كان غير مسجل ضمن قائمة إتصال المرسل إليه.	العميلة السلوفينية، حيث يظهر اسم المرسل أعلى النص مكتوب باللغة الإنجليزية (-----) بعد كلمة (:From).

العناصر الداخلية	رسالة البريد الصادرة	رسالة البريد الواردة
المرسل إليه (الموجهة إليه الرسالة)	العميلة السلوفينية، حيث يظهر اسم المرسل إليه أعلى النص مكتوب باللغة الإنجليزية بعد كلمة (To:)	(عنوان البريد الإلكتروني المزور لمدير تصدير شركة ------ للملابس الجاهزة) heshamamer@heshamtex.com وهو مكتوب باللغة الإنجليزية في أعلى الرسالة بعد كلمة (To:)
الدولة التابع لها	مصر	دولة سلوفينيا
تاريخ الإرسال	2013/4/16 وهو مدون على شمال اسم المرسل بأعلى الصفحة باللغة الإنجليزية.	2013/4/16 وهو مدون على شمال اسم المرسل بأعلى الصفحة باللغة الإنجليزية
الموضوع	جاء ذكر الموضوع مكتوب في أعلى الرسالة باللغة الإنجليزية (In: sent)، وهو يعني أن موضوع الرسالة هو رسالة مرسلة إلى المجني عليه.	جاء ذكر الموضوع مكتوب في أعلى الرسالة باللغة الإنجليزية (RE: Request)، وهو يعني أن موضوع الرسالة هو الرد على الرسالة المرسلة من الجاني.
وصف الحدث	رسالة مرسلة إلى العميلة السلوفينية بالخارج لطلب إرسال مبلغ مالي قدره 3200 يورو (ثلاثة آلاف ومائتي يورو) وهو باقي ثمن شراء صفقة (بشاكير بحر) كانت قد قامت بشرائها من شركة ------ للملابس الجاهزة ، وذلك إلى رقم حساب شركة تو ام (tow.m) بالبنك الوطني المصري فرع الحجاز، بدعوى أنه حساب بديل خاص بالشركة بدلاً من الحساب الحقيقي الذي يتم التعامل معه وهو رقم حساب خاص بالمتهم الأول.	رسالة مستلمة من العميلة السلوفينية عبارة عن صورة استمارة تحويل مبلغ 3200 يورو من بنك NLB في سلوفينيا إلى حساب المتهم الأول (شركة تو ام (tow.m) بالبنك الوطني المصري فرع الحجاز).

العناصر الداخلية	رسالة البريد الصادرة	رسالة البريد الواردة
أهلية التوقيع	جاء في البروتوكول الختامي للرسالة، حيث ذُكرت بيانات الوظيفة بعد اسم المرسل. (مدير تصدير شركة ------- للملابس الجاهزة).	جاء في البروتوكول الختامي للرسالة، حيث ذُكرت بيانات الوظيفة بعد اسم المرسل. (مندوب شركة ------ باسم -- ------).

جدول رقم (9) يوضح العناصر الداخلية لرسالة (وثيقة) البريد الإلكتروني الصادرة والواردة

العناصر الداخلية لرسائل الهاتف المحمول الصادرة والواردة:

المسئول (المرسل): ------ وهو الإسم الحركي للمتهم الثالث، وهو مدون باللغة الإنجليزية في أعلى نص الرسالة ------- مدون أسفل الإسم رقم التليفون.

المرسل إليه (الموجهة إليه الرسالة): المتهم الأول (----------).

الدولة التابع لها: نيجيريا

تاريخ الإرسال: 2013/4/16 وهو مدون أعلى الرسالة باللغة الإنجليزية

الموضوع: رسائل واردة وصادرة بين الطرفين

وصف الحدث: تحتوي تلك الرسائل على بيانات بنكية بين الطرفين مرفق بها صورة استمارة تحويل مبلغ 3200 يورو من بنك NLB في سلوفينيا إلى حساب المتهم الأول (شركة تو ام (tow.m) بالبنك الوطني المصري فرع الحجاز).

ACC NAME OF COMPANY: TOW.M.

ACC.NO.: 229447

BANK NAME: ABC BANK

BANK SWIFT CODE: EAABEGCXXXX

BANK BRANCH: KATAMIAH BRANCH

BANK ADRESS: FIFTH AVENUE. CAIRO EGYPT

كما تحتوي تلك الرسائل على اتفاق بين الطرفين على مكان التقابل ومعرفة نسبة الربح والتي قدرها المتهم بـ10% إلى 15 %[130].

[130] وثائق قضية جنحة رقم 844 لسنة 2013 جنح اقتصادية القاهرة.

يتضح مما سبق، أن تحليل العناصر الخارجية والداخلية لأدلة إثبات تزوير البريد الإلكتروني (لمدير تصدير شركة -------) وفقا لمنهج علم الدبلوماتيك الرقمي مطابقاً لما يقوم به خبراء الفحص الجنائي الرقمي، حيث يمكن من خلال هذا التحليل تحديد الجاني والمجني عليه والحدث الذي شاركت فيه وثيقة البريد الإلكتروني ورسائل الهاتف المحمول وتواريخ الإنشاء.

د) التداول (مرحلة تدوين النتائج وإعداد التقرير):

تتضمن هذه المرحلة وفقاً للإثبات الجنائي إعداد التقارير عن الأنشطة والفحوص التي تمت، وتدوين النتائج. وذلك من واقع أدلة الثبوت التي أوردتها سنداً لهذا الاتهام والمتمثلة في شهادة مدير الشركة المجني عليها في تحقيقات النيابة العامة وما قرره بالاستدلالات والتي تأيدت بتحريات الشرطة وشهادة مجريها، ومما ثبت من التقرير الفني. وتتمثل هذه المرحلة في إعداد محاضر التحريات والضبط والتفتيش وتقرير الفحص الفني وتقديمها للنيابة العامة.

هـ) مر اقبة التداول (تقديم حزمة الأدلة):

تتمثل هذه المرحلة وفقاً للإثبات الجنائي، في قيام النيابة العامة بتقديم جميع أوراق القضية لمحكمة جُنح النزهة الجزئية والتي قضت بعدم اختصاصها نوعياً بنظر الجنحة وأحالتها للنيابة العامة مرة أخرى لإرسالها للمحكمة الاقتصادية. ونفاذاً لذلك القضاء أُحيلت الأوراق لهذه المحكمة، وتداولت بالجلسات على النحو الثابت بمحاضرها، وقد مثُل المتهمين جميعاً ومعهم (محام)، وانتدبت المحكمة مترجماً للغة الإنجليزية لتعذر سؤال المتهمين الأجانب عن الاتهام المنسوب إليهم.

و) التنفيذ (إدارة مواد القضية):

تُشير هذه المرحلة وفقاً للإثبات الجنائي إلى التأكد من توافر الركن المادي والمعنوي لارتكاب الجريمة، يتحقق الركن المادي في قيام المتهمين باصطناع بريد إلكتروني نسبوه زوراً إلى المجني عليه واستخدموه بغية الإضرار به وهو ما يمثل الركن المادي للجرائم المسندة للمتهمين، وتحقق كذلك الركن المعنوي للجريمة وهو علمهم بمباشرة النشاط الإجرامي محل الركن المادي واتجاه إرادتهم إلى تحقيق ذلك، وعليه فقد استخلصت المحكمة أن المتهمين اتجهت إرادتهم الآثمة عن طواعية وحرية اختيار إلى اقتراف الاتهامات المسندة إليهم، مما يثبت معه توافر أركان الجرائم في حقهم، وفقاً لأحكام المادة (23) من قانون التوقيع الإلكتروني المصري، وعملاً بنص المادة 2/304 من قانون الإجراءات الجنائية.

كما تتضمن مرحلة التنفيذ وفقاً للإثبات الجنائي وثيقة النطق بالحكم أول درجة ضد المتهمين، ولما كان من الثابت بورقة الحكم أن الهيئة التي استمعت للمرافعة وتداولت في إصدار الحكم أنها وقعت أسبابه ومنطوقه فإنه يكون سليماً وبمنأى عن البطلان[131]. وقد ترتب على هذه المرحلة عدة إجراءات فرعية، حيث طعن المتهمون على هذا الحكم بطريق الاستئناف، ولما كان الاستئناف مستوفياً لأوضاعه الشكلية المقررة قانوناً فقد تم قبوله شكلاً.

أما عن موضوع الاستئناف فقد اطمئنت المحكمة إلى ثبوت الاتهام في حق المتهمين الأول والثالث، حيث أن أدلة الثبوت محصورة بينهما فالمتهم الأول هو من تلقى المبلغ المستولى عليه على حسابه بالبنك الوطني فرع الحجاز والذي أمد به المتهم الثالث الذي قام باستعمال الطرق الاحتيالية للتوصل إلى الاستيلاء على هذا المال، وذلك من اختراق البريد الإلكتروني للشركة المجني عليها، وتزوير عنوان هذا البريد.

أما بشأن ما نُسب إلى باقي المتهمين وهم الثاني والرابع والخامس والسادس فإن المحكمة ترى أن الدليل على ارتكابهم للواقعة موضوع الاتهام جاء قاصراً عن بلوغ حد الكفاية لاقتناعها بثبوت ذلك الاتهام وصحة إسناده إليهم، إذ أن هذا الدليل جاء محصوراً في تحريات الشُرطة التي هي مجرد رأي لمجريها ولا تصلح وحدها دليلاً على الإدانة وخلت الأوراق من بعد من دليل آخر يقيني يصلح سنداً لإدانتهم الأمر الذي يتعين معه إلغاء الحكم المستأنف فيما قضى به بالنسبة لهؤلاء المتهمين والقضاء ببرائتهم مما أُسند إليهم طواعية لنص المادة 1/304 من قانون الإجراءات الجنائية[132].

3 - السياق القانوني:

يظهر السياق القانوني في الحكم الصادر من المحكمة ضد المتهمين، ووفقاً للحكم الصادر فقد تمت معاقبة المتهمين وفقاً لأحكام المواد 23/ (ب)، 23/ (ج)، 23/ (هـ) من قانون تنظيم التوقيع الإلكتروني المصري رقم 15 لسنة 2004، وعملاً بنص المادة 2/304 من قانون الإجراءات الجنائية مع إلزامهم بالمصروفات عملاً بنص المادة 313 من قانون الإجراءات الجنائية.

---

[131] وثائق قضية جنحة رقم 844 لسنة 2013جنح اقتصادية القاهرة.

[132] انظر الملحق السادس من رسالة حسناء على على عبد الغني. (2022)، (وثائق قضية جنحة رقم 301 لسنة 2013جنح مسأنف ورقم 844 لسنة 2013جنح اقتصادية القاهرة)، ص 341 - 346.

والجدول رقم (10) يوضح مدى مطابقة السياق القانوني للأحكام القضائية الصادرة بشأن هذه الدعوى الجنائية (تزوير عنوان البريد الإلكتروني):

الإتهام	السياق القانوني للدعوى الجنائية	الحكم
- تزوير عنوان البريد الإلكتروني الخاص بالمجني عليه[133].	تنص المادة 23/ (ب)، 23/ (ج)، 23/ (هـ) من قانون تنظيم التوقيع الإلكتروني المصري رقم 15 لسنة 2004 على أنه: "مع عدم الإخلال بأية عقوبة أشد منصوص عليها في قانون العقوبات أو في أي قانون آخر، يُعاقب بالحبس وبغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز مائة ألف جنيه أو بإحدى هاتين العقوبتين كل من: 23/ ب – أتلف أو عيب توقيعاً أو وسيطاً أو محرراً إلكترونياً، أو زور شيئاً من ذلك بطريق الاصطناع أو التعديل أو التحوير أو بأي طريق آخر. **23/ج-** استعمل توقيعاً أو وسيطاً أو محرراً إلكترونياً أو زور شيئاً من ذلك بطريق الإصطناع أو التعديل أو التحوير أو بأي طريق آخر. **23/ هـ -** توصل بأية وسيلة إلى الحصول بغير حق على توقيع أو وسيط أو محرر إلكتروني، أو اخترق هذا الوسيط أو اعترضه أو عطله عن أداء وظيفته. وفي جميع الأحوال يحكم بنشر حكم الإدانة في جريدتين يوميتين واسعتي الانتشار، وعلى	قضت محكمة أول درجة / بحبس المتهمين سنة مع الشُغل، وتغريمهم عشرة آلاف جنيهاً والمصاريف والزامهم بنشر الحكم في جريدتي الأهرام والأخبار، وعلى شبكات المعلومات الإلكترونية المفتوحة على نفقة المحكوم عليهم[135]. أما محكمة الاستئناف فقد قضت بتأييد الحُكم المستأنف فيما قضى به على المتهمين الأول والثالث وألزمتهما بالمصاريف وبإلغاء الحُكم المستأنف فيما قضى به بالنسبة للمتهمين الثاني والرابع والخامس والسادس

[133] قضية جنحة رقم 844 لسنة 2013 جنح اقتصادية القاهرة.

[135] قضية جنحة رقم 844 لسنة 2013 جنح اقتصادية القاهرة.

الإتهام	السياق القانوني للدعوى الجنائية	الحكم
	شـبكات المعلومات الإلكترونية المفتوحة على نفقة المحكوم عليه[134].	وببراءتهم ممـا أُسـنـد إليهم[136].

يتضح من الجدول السـابق أنه عند مقارنة نصـوص القوانين بالتهم المبينة بالدعوى الجنائية، تبين أنَ الحكم القانوني الصـادر بشـأن هذه الدعوى الجنائية يتم وفقاً للقوانين المنصوص عليها في وثائق القضية.

4 - السياق التقني:

قـامت إدارة مكافحـة جرائم التزييف والتزوير بفحص أجهزة الحاسـب الآلي التي تم ضـبطها، وتبين أن جهازي الحاسـب الآلي ماركة سـامسـونج تم حمايتهما بكلمة مرور ولم تتمكن الإدارة من فحصـها. أما بالنسـبة لجهاز الحاسـب الآلي ماركة آسـر (Acer) تبين وجود أحد برامج القرصـنة عليه، حيث يُمَكِن مسـتخدمه من التخفي عبر الإنترنت من خلال اسـتخدام رقم تعريفي خاص بآخرين من دول غير الدولة التي يدخل منها على الإنترنت وهو أحد أسـاليب الهاكر الشهيرة، كما عثر على ملف بصيغة Pam.txt يحتوي على نصوص لرسائل احتيالية [137] يتم إرسـالها للأشـخاص بشـكلٍ عشـوائي، كذلك عُثر على ملفٍ آخر باسـم arabooooooo. txt وهو يحتوي على نصوص رسائل احتيالية مماثلة لمحتويات الملف السابق.

---

[134] قانون التوقيع الإلكترونى المصرى رقم 15 لسنة 2004، المادة 23/ (ب)، 23/ج، 23/ (هـ) .

[136] انظر الملحق السادس من رسالة حسناء على على عبد الغني. (2022)، (وثائق قضية جنحة رقم 301 لسنة 2013جنح مسأنف ورقم 844 لسنة 2013جنح اقتصادية القاهرة)، ص 341 - 346.

[137] **الرسـائل الاحتيالية Phishing mail**: وتسـمى رسـائل التصـيد، وهى: (سـرقة المعلومات الشـخصـية عن طريق انتحال شخصية أو مؤسسة موثوقة، وتستخدم بشكل عام لغرض سرقة الهوية).

التصيد Phishing - أي عملية اكتساب معلومات سرية مثل أسماء المستخدمين وكلمات المرور وبيانات بطاقة الائتمان - شـكل جديد وشـائع جدا من أشـكال الاحتيال التي تتم من خلال البريد الإلكتروني وسـمى هذا النوع من الرسـائل "رسـائل الاصـطياد الإلكترونى"، لأن مرسـلها يسـتخدم رسـائل البريد الإلكترونى كطعم لإصـطياد الأرقام السـرية وغيرها من البيانات الشـخصـية الحسـاسـة الأخرى من مسـتخدمى شـبكة الإنترنت.ومن الأمثلة على هذا النوع من الرسائل، رسالة بالبريد الإلكترونى من موظفى البنك الذى يتعامل معه المسـتقبل، أو من موقع إلكترونى يطلب منه تحديث معلومات سـرية، أو تأكيد معلومات البطاقة الائتمانية، وبذلك يقع المسـتلم ضـحية لسـرقة ارقامه السـرية وهويته الخاصـة. انظر: عائشـة حلمي. (2018). نفس المرجع، ص 201-202.

ويتضح من فحص الجهاز آنف البيان قيام صاحبه بالاحتيال على الآخرين عبر البريد الإلكتروني بزعم أنه صاحب البيانات التي تحويها نصوص الرسائل كما يمكنه زعم أنه مقيم بأي دولة يمكنه تحديدها واستخدام رقم تعريفي يخص تلك الدولة.

وبفحص جهاز الحاسب الآلي المحمول ماركة HP موديل Pavilion 96 تبين أنه يحمل ملفات بصيغة ARAB,YTY,TXT,PAM,TXT، وجميعها تحتوي على نصوص يتم استخدامها في رسائل البريد الخادعة للاحتيال على الأشخاص كما عثر على برنامج HIDE MY ASS PRO VPN وهو ذات البرنامج الذي يستخدم لإخفاء الرقم التعريفي.

وبفحص حرز الهواتف المحمولة المدون عليه اسم المتهم تبين احتواؤه على عدد جهازي هاتف محمول أحدهما ماركة blackberry أسود اللون Curve والآخر ماركة G-TIDE موديل G707.[138]

ويُعتبر ما قامت به إدارة مكافحة جرائم التزييف والتزوير مطابقاً لمنهج علم الدبلوماتيك الرقمي. إلا أنه وفقاً لفهمه كان يجب فحص سجلات الدخول للبريد الإلكتروني وفحص ميتاداتا الملفات ونظام البريد الإلكتروني للكشف عن أي تناقضات في الميتاداتا أو النظام.

- **الوسيط :** شريحة الهاتف المحمول والمسجلة باسم المتهم وعنوانه .

والجدول رقم (11) يوضح مدى مطابقة الفحص الجنائي الرقمي لمنهج علم الدبلوماتيك الرقمي في جريمة تزوير البريد الإلكتروني:

وجه المقارنة	الفحص الجنائي الرقمي	عناصرالنقد (الفحص) الدبلوماتي الرقمي	مطابق	غير مطابق
الخصائص الخارجية	فحص عنوان البريد الإلكتروني وكلمة المرور الخاصة به وفحص صيغ الملفات وبرامج القرصنة	الخصائص الخارجية (خصائص العرض)	مطابق	
الخصائص الداخلية	فحص محتوى الرسائل الصادرة والواردة	الخصائص الداخلية	مطابق	غير مطابق

[138] قضية جنحة رقم 844 لسنة 2013 جنح اقتصادية القاهرة.

وجه المقارنة	الفحص الجنائي الرقمي	عناصرالنقد (الفحص) الدبلوماتي الرقمي	مطابق	غير مطابق
	تحديد عنوان IP الخاص بكل رسالة وتحديد المرسل	المسؤول عن التزوير(الجاني)	مطابق	
	تحديد المرسل إليه	المجني عليه	مطابق	
	تحديد تاريخ الإرسال	التاريخ الزماني	مطابق	
	تحديد الموقع الجغرافي للجهاز الذي حدثت العملية من خلاله	التاريخ المكاني	مطابق	
	تحديد الموضوع الذي شاركت فيه الوثيقة	وصف الحدث	مطابق	
الوسيط	فحص شريحة الهاتف المحمول	الوسيط	مطابق	
السياق	تتبع الرقم التعريفيIP	سياق المصدر	مطابق	
	تحديد إجراءات الإثبات الجنائي	سياق الإجراءات	مطابق	
	تحديد الإطار القانوني الذي تتم فيه الدعوى الجنائية	السياق القانوني	مطابق	
	الفحص الفني لمكونات ومحتويات جهاز الحاسب الآلي والهواتف المحمولة	السياق التقني	مطابق	

الجريمة الر ابعة: سرقة توقيع الوسيط الإلكتروني (صفحة حساب الفيس بوك الخاص بالمجني عليها) [139]

يعتبر الفيس بوك من أشهر مواقع التواصل الاجتماعي Social Media، التي تسمح للمستخدم ليس فقط بالوصول إلى المحتوى على الإنترنت، بل بتحرير المحتوى وتحميله والتعليق عليه وتعديله. ومن أهم مواقع التواصل الاجتماعي: فيس بوك وتويتر وواتس اب، ولينكد إن.

[139] قضية جنحة رقم 307 لسنة 2017 جنح اقتصادية القاهرة.

وتُعرف مواقع التواصـــل الاجتماعي بـأنها مجموعـة من التطبيقـات المعلوماتيـة على الإنترنت ترتكز على أيدولوجيات ومبادئ الويب والتي تسـمح بإنشـاء ومشـاركة المحتوى من قبل المستخدمين[140].

ومما لا شـك فيه أنَ وجود مواقع التواصـل الاجتماعي social media في كل مكان، وفي جميع الأوقات، وحجم المعلومات الشـخصـية التي تحتويها هذه المواقع، يجعل منها مصـدراً خصباً وغنياً للأدلة المحتملة التي يمكن أن تستخدم في الإجراءات الجنائية. وبالنظر إلى طبيعة هذه المواقع، فإنها تُثير تحديات كبيرة، يتعلق بعضـها بالمصـداقية التي تتمتع بها الأدلة الناتجة عن هذه المواقع[141]، لذلك لكي يكون للوثائق الناتجة عن مواقع التواصـل الاجتماعي حجية أمام القضاء يجب التعرف على طبيعتها الوثائقية، وهنا تظهر أهمية علم الدبلوماتيك ودوره في التعرف على طبيعة الوثائق (الأدلة) الرقمية من خلال فحص مكونات الكيان الرقمي للتأكد من كونه وثيقة أم لا ثم اسـتخراج عناصـر النقد الدبلوماتي للحكم على صحة الوثيقة أو عدم صحتها.

التحليل الدبلوماتي الرقمي لمو اقع التواصل الاجتماعي كوثائق تفاعلية ديناميكية:

نظراً لأن الفيس بوك والو اتس اب من أشـــهر مو اقع التواصـــل الاجتماعي، والتي تعتبر مصـدراً خصـباً وغنياً للوثائق (الأدلة) التفاعلية الديناميكية التي يمكن أن تسـتخدم في الإجراءات الجنائية، لذلك وفقاً للدبلوماتيك الرقمي قبل الشـروع في اسـتخراج عناصـر النقد يجب فحصهما أولاً للتأكد من كونهما وثيقة أم لا، وذلك بالبحث عن المكونات الست للوثيقة:

أولاً- المحتوى:

يعتبر برنامج الفيس بوك والواتس اب مثالاً على الوثائق التفاعلية، والتي يتغير فيها المحتوى وفقاً لمدخلات المُسـتخدم، كما يُعتبر الفيس بوك أشـهر مواقع الويب الديناميكية، حيث يسـمح للمسـتخدم بالإضـافة والحذف والتعديل في أي وقت يشـاء، دون إحداث تأثير في

---

[140] Coe, P. (2015). The social media paradox: an intersection with freedom of expression and the criminal law. *Information & Communications Technology Law, 24*(1), p2.

[141] سامي حمدان الرواشده.(2017). الأدلة المتحصلة من مواقع التواصل الإجتماعي ودورها في الإثبات الجنائي: دراسة في القانونين الإنجليزي والأمريكي. المجلة الدولية للقانون، 14 (3)، ص1. متاح على الرابط التالي: https://www.qscience.com/docserver/fulltext/irl/2017/3/irl.2017.14.pdf? (last visited 23/2/2020).

الخصـائص المادية أو التقنية للوثيقة، لذلك يجب على الدبلوماتي التأكد من سـلامة المحتوى واسـتقراره. ويتراوح المحتوى ما بين رسـائل نصـية، إلى صـور يتم تبادلها، ومقاطع فيديو وموسيقى تحظى بمشاهدات كثيرة.

تتم حماية الحسابات على الفيس بوك وواتس اب بكلمات مرور Password، ويستطيع المسـتخدم تحديد مسـتوى الخصـوصـية للحسـاب كله أو جزء منه؛ فالمحتوى يمكن أن يكون خاصاً أو عاماً أو متوفراً لمجموعة من الأصدقاء فحسب. ويعتمد مدى الحماية ومستواها على مزود خدمة الفيس بوك والواتس اب[142]. ويتم تخزين كافة الإتصـالات التي يتم إرسـالها من خلال مزود شبكة الفيس بوك، وكافة المعلومات التي يتم تحميلها على الحسابات الموجودة على هذه المواقع، على الخوادم (Servers) التي تكون موجودة في الخارج عادة . ويُعد هذا أحد مظاهر الحوسـبة السـحابية، والتي تعمل من خلالها معظم مواقع التواصـل الاجتماعي[143]. إذا ما قام المُسـتخدم بإنشـاء حسـاب على أحد مواقع التواصـل الاجتماعي، فإن الموقع سـيسـجل عنوان بروتوكول الإنترنت IP Address، وبناءً على ذلك، فإن المعلومات المتعلقة ببروتوكول الإنترنت المخصصة لأي جهاز حاسب آخر يستخدمه الفرد من أجل الدخول إلى حسابه على الفيس يتم تسجيلها. ويمكن طلب تسجيلات الأنشطة التي يُستقى منها عنوان بروتوكول الإنترنت من موقع التواصـل الاجتماعي فيس بوك، وتكشـف هذه التسـجيلات كل الاتصـالات والحركات التي تمت من قبل المسـتخدم،[144] وكل هذه المعلومات يتم تسـجيلها في خادم الموقع، فإذا قام أحد الأشخاص بإرسال رسالة من حسابه الشخصي على الموقع إلى شخص آخر، فإن هذه الرسالة

---

[142] Waterloo, S. F., Baumgartner, S. E., Peter, J., & Valkenburg, P. M. (2018). Norms of online expressions of emotion: Comparing Facebook, Twitter, Instagram, and WhatsApp. *new media & society*, *20*(5), 1813-1831. Retrieved from: https://journals.sagepub.com/doi/pdf/10.1177/1461444817707349 (last visited 19/1/2021)

[143] Walden, I. (2013). Accessing data in the Cloud: The long arm of the Law Enforcement Agent. In *Privacy and Security for Cloud Computing* (pp. 45-71). Springer, London. Retrieved from: http://www.wikayanet.dz/images/Documentation/Livres/PrivacySecurityCC.pdf (last visited 19/1/2021).

[144] Brandtzaeg, P. B., & Heim, J. (2009, July). Why people use social networking sites. In *International conference on online communities and social computing* (pp. 143-152). Springer, Berlin, Heidelberg.

سـوف تُخزن في حسـاب الشـخص الآخر على الخادم الخاص بالموقع، كذلك من الممكن تخزين المعلومات على ذاكرة جهاز الحاسب المملوك للمستخدم، ويعتمد هذا إلى حد كبير على سياسة الخصـوصـية المعتمدة من قبل الموقع ذاته، وعلى متصـفح الإنترنت الذي يسـتعمله المسـتخدم للولوج إلى الموقع. ولذلك، فإن تحليل القرص الصـلب الموجود في الحاسـب يؤدي في بعض الأحيان إلى الكشف عن محتوى الاتصالات التي تمت على موقع التواصل.[145]

والخلاصـة، أنه على الرغم من أن مواقع التواصـل الاجتماعي (الفيس بوك والواتس اب) تسـمح للمسـتخدم بالإضـافة والحذف والتعديل في أي وقت يشـاء، إلا أنه يشـترط عدم إحداث تأثير في الخصـائص المادية أو التقنية للوثيقة، بالإضـافة إلى أن النظام يحتفظ بالمراسـلات التي يتم إرسـالها أو اسـتقبالها، وبالتالي يمكن تقديم الرسـالة أو محتوى الرسـالة بنفس العرض الوثائقي المقدم على الشـاشـة عند حفظه أول مره، والذي بدوره يُسـاعد في التحقق من أصالة المحتوى والتأكد من عدم تغييره.

ثانياً - الشكل

الشـكل الثابت يتكون من جوانب الشـكل الذي يقوم بتحديده المسـئول عن إعداد الوثائق أو التحكم فيها[146]، ويشـمل ثبات الشـكل في مواقع الفيس بوك والواتس اب الجوانب التي تظهر دائماً في المواقع مهما تغير المحتوى، مثل: واجهة الموقع، وقائمة الأصـدقاء، وعضـوية المجموعات، والرسـائل، وسـجلات المحادثات، والتغريدات، والصـور، ومقاطع الفيديو، ووضـع العلامات، ونظام تحديد المواقع، والإعجابات، وتسـجيل الدخول إلى أحد الأماكن.[147] كما يشـمل الجوانب التي تحدد كيف يتم عرض المحتوى وفقاً لمدخلات المسـتخدم مثل، الحجم وموضع الصور في النص وعرض بعض البيانات في نافذة جديدة[148]. كذلك يعتمد الفيس بوك على إنشاء تطبيقات تتفاعل مع خصائصه الأساسية[149].

---

(145) O'Floinn, M., & Ormerod, D. (2011). Social networking sites, RIPA and criminal investigations. *Criminal Law Review*, *2011*(10), 766-789.

(146) دينا محمود عبد اللطيف. نفس المرجع، ص 291.

(147) Larsson, A. O. (2018). The news user on social media: A comparative study of interacting with media organizations on Facebook and Instagram. *Journalism studies*, *19*(15), 2225-2242.

(148) دينا محمود عبد اللطيف. نفس المرجع، ص 291.

(149) Waterloo, S. F., Baumgartner, S. E., Peter, J., & Valkenburg, P. M. (2018). op.cit,P 1813-1831.

ويتضح مما سبق، أنه على الرغم من أن القواعد التي تنظم المحتوى وشكل العرض لمواقع التواصل الاجتماعي (الفيس بوك والواتس اب) متغيرة، إلا أنه يمكن اعتبار الأدلة الناتجة عنها وثائق دبلوماتية تستحق النقد، وذلك للأسباب التالية:

- يتم تخزين الأصول الرقمية (كافة الاتصالات التي يتم إرسالها من خلال شبكات مواقع التواصل الاجتماعي، وكافة المعلومات التي يتم تحميلها على الحسابات الموجودة على هذه المواقع) يومياً على شرائط النسخ الإحتياطي والاحتفاظ بها على خوادم الحوسبة السحابية[150] DHL، التي توجد في قسم التكنولوجيا.

- في حالة حذف أو تغيير المنشور على صفحة الفيس بوك فإنه يتم حفظه في شكل ثابت داخل نظام الفيس بوك، مثل: أخذ صورة سكرين شوت Screen shot من مقطع فيديو، على الرغم من أن الصورة تفتقد للحركة إلا أنها تُسجل الواقعة. وفي هذه الحالة حتى لو فقدت الصورة ديناميكيتها، إلا أنها تُفيد في بعض الحالات كمراجعة شكل الوثيقة في حالة الحفظ، كما أنه يمكن الرجوع إلى ميتاداتا حفظ هذه الكيانات للتثبت من صحتها. كما يمكن حفظ الرسائل المتبادلة على وسائل التواصل الاجتماعي بشكلٍ شبه دائم. ومن هنا يمكن القول أن الشكل الوثائقي والمحتوى للأصل الرقمي ثابت، حيث يتم وصف كل منها بدقة لأغراض استرجاعها وحفظها من خلال الميتاداتا الوصفية.

- يعتمد الفيس بوك على إنشاء تطبيقات تتفاعل مع خصائص الفيس بوك الأساسية، مما يعني أن التنوع في الشكل يكون محدوداً ولا يؤثر على الخصائص المادية للوثيقة، ومن هنا يمكن القول أن النظام قادر على إعادة إنتاج ما تم حفظه بنفس الشكل والمحتوى مرة أخرى، لذلك يجب على الدبلوماتي معرفة خصائص النظام الذي يقوم بعرض الوثائق لأن كل نظام له طريقة محددةً لعرض وثائقه.

ثالثاً - الحدث

لابد للوثيقة أن تُشارك في حدث ما، وقد أصبح أمراً اعتيادياً الإعتماد على أدلة ناتجة عن الفيسبوك وغيره من مواقع التواصل الإجتماعي، حيث تُشكل بعض الإتصالات في مواقع التواصل الإجتماعي جريمة يعاقب عليها القانون. ولم يعد سراً القول أنَ أجهزة العدالة

[150] لمزيد من التفاصيل حول الحوسبة السحابية. انظر: حسناء علي علي. (2018). المعيار الدولي أيزو/ 17068، ص 86 – 93.

الجنائية تقوم بتفتيش مواقع التواصل الإجتماعي بحثاً عن أدلة، وبدون الحاجة للحصول على تفويض من المحكمة أو طلب إحضـــار، هناك الكثير من المعلومات المهمة المتمثلة في الأدلة المتوفرة للعامة على مواقع التواصـــل الإجتماعي. يكون لهذا النوع من الأدلة – عادة – تأثير كبيرعلى المحكمة وهيئة المُحلفين، فالدليل قد يكون عبارة عن تصـــوير أو رســـم يمثل كلمات مطبوعة أو صوراً تم تحميلها على مواقع إلكترونية من قبل الأشخاص المعنيين بالمحاكمة، وهم تحديداً: المتهمون، والمشـــتكون، والشـــهود وبناءً على ذلك، يجب أن تكون تلك الأدلة واضـــحة وقائمة على أسس قانونية، هي: أن تتمتع بالأصالة، وتتعلق بالوقائع المراد إثباتها، ويجوز قبولها في الإثبات.[151]

ويجب الإشارة إلى أنَ مواقع التواصل الإجتماعي مثل فيسبوك قادرة على تزويد أجهزة الشرطة والنيابة العامة والقضاء بمعلوماتٍ كاملة عن صاحب الحساب، إضافة إلى المراسلات الموجودة على واجهة الموقع، والصور التي يتم تحميلها على الموقع، والصور التي تم التأشير عليها من قبل المســتخدم، وقائمة شــاملة بالأصــدقاء، وعمليات تسـجيل الدُخول، ومعلومات تحديد الموقع بدقة[152].

رابعاً – الأشخاص

- **الفيس بوكFacebook**

المســئول عن الفيس بوك هو مارك زوكربيرج Mark Zuckerberg، وهو رئيس مجلس إدارة شركة الفيس بوك والمدير التنفيذي لها.

- **الواتس اب**

المسـئول عن الواتس اب هو ويل كاثكارت Will Cathcart، وهو مدير شـركة واتس اب والمتحدث الرسمى باسم الشركة.

خامساً – السياق

1 - السياق القانوني للفيس بوك والواتس اب

تعمل مواقع التواصل الإجتماعي (فيس بوك، واتس اب) وفقاً لقوانين حماية البيانات الشخصية للمستخدمين وقوانين أمن المعلومات.

---

[151] سامي حمدان الرواشده.(2017). الأدلة المتحصلة من مواقع التواصل الإجتماعي، ص2-4.

[152] Parascandola, R. NYPD Forms New Social Media Unit to Mine Facebook and Twitter for Mayhem. The New York Daily News, August 10, 2011, p 4.

2 - سياق المصدر للفيس بوك والو اتس اب

- الفيس بوك

أطلق مارك زوكربيرج Mark Zuckerbergموقع الفيس بوك في عام 2004، وهو رجل أعمال ومبرمج أميركي، وُلد في وايت بلينس، نيويورك، الولايات المتحدة الأمريكية. اشتهر بتأسيسه موقع التواصل الاجتماعي فيس بوك، وهو أكبر موقع تواصل اجتماعي في العالم، أنشأ الموقع مع زملائه في قسم علوم الحاسب (جامعة هارفارد) أندرو ماكولوم، وإدواردو سفارين، وداستن موسكوفيتز وكريس هيوز. وقد تم فتح الفيس بوك للعموم في عام 2005، بعد تأمين التمويل اللازم للتوسع، وأصبح كل شخص له بريد إلكتروني مرتبط بمؤسسة الحق بالعضوية في الفيس بوك. وفي عام 2006، تم فتح الفيس بوك لكل مستخدم له عنوان بريد إلكتروني صحيح. وفي عام 2007، أعلن زوكربيرج أن فيس بوك سيصبح النظام التشغيلي الاجتماعي للإنترنت، وأصبح بإمكان المستخدمين دمج نشاطاتهم على الإنترنت عبر سيرتهم على فيس بوك، ولم تعد المنصة التقنية لفيس بوك وحده. وفي عام 2007، قدَم فيس بوك للمعلنين وصول مباشر للمستهلكين المستهدفين[153].

ويتطلب الفيس بوك من المستخدمين وضع هوياتهم الحقيقية ومعلوماتهم الشخصية الصحيحة وعدم إنشاء حسابات وهمية، وهو ما يُعرف بمبدأ التعريف Identity. ويبقى المحتوى الموضوع من المُستخدم على فيس بوك موجود إلى حين إزالته من قبل المُستخدم نفسه أو من قبل المسئول عن الفيس بوك، وهو ما يُعرف بمبدأ الدوام Permanence. أسندت فيس بوك مهمة إدارة المحتوى المنشور عليه إلى شركة خاصة هي شركة (oDesk). وتقوم الشركة المذكورة عبر العاملين لديها بمراجعة يومية للمحتوى على فيس بوك، للتأكد من عدم وجود انتهاك لسياسات ولمعايير الموقع[154].

---

[153] Croft, C. (2007). A brief history of the Facebook. *Retrieved from.* http://www.meerutcollege.org/mcm_admin/upload/1587223450.pdf (last visited 23/1/2021).

[154] Steppe, R. (2014). The freedom of speech on social networking services-Do we need protection against our own expressions?. *Jura Falconis, 2013*(3), p563.

- **الواتس اب**

يُعتبر تطبيق الواتس اب WhatsApp أكبر تطبيق للرسائل على الإنترنت، وقد تأسس في عام 2009م، من قبل موظفي ياهو (Yahoo) السابقين، وهم جان كووم Jan Koum، وبريان أكتون Brian Acton. وقد كانت واتس اب في بدايتها خدمة مدفوعة تفادياً لارتفاع عدد المُستخدمين، لأن التطبيق حينها كان لا يتحمل عدد كبير من المُستخدمين. وقد استحوذت فيس بوك على واتس اب عام 2014، إلا أن الأخيرة لا تزال تعمل كتطبيق معلوماتي مستقل. وفي عام 2015 أدخلت واتس اب تطبيق معلوماتي على جوجل كروم (Whatsapp Web) للسماح للمستخدمين بالوصول إلى رسائلهم من خلال الحاسبات الشخصية. كما يسمح هذا التطبيق بالوصول إلى رسائل هاتف المستخدم أيضاً[155].

3 - السياق التوثيقي للفيس بوك والواتس اب

يرتبط الفيس بوك ببعض المواقع الأخرى مثل يوتيوب وتويتر وانستجرام والواتس اب، حيث يقوم بمشاركة منشورات وأخبار من هذه المواقع. كما يرتبط الواتس اب بجوجل كروم وببعض المواقع الأخرى مثل فيس بوك ويوتيوب وغيرها من المواقع التي يمكنها مشاركة منشوراتها وأخبارها عبر الواتس اب.

4 - السياق التقني للفيس بوك والواتس اب

- **<u>الفيس بوك</u>**

يتضمن فيس بوك عددًا من التطبيقات التي تتيح للمستخدمين إمكانية التواصل مع بعضهم البعض، ومن بين هذه التطبيقات:

- **تطبيق <u>Wall</u>** أو لوحة الحائط وهو عبارة عن مساحة مخصصة في صفحة الملف الشخصي لأي مستخدم بحيث تتيح للأصدقاء إرسال الرسائل المختلفة إلى هذا المستخدم.

(155) Church, K., & De Oliveira, R. (2013, August). What's up with WhatsApp? Comparing mobile instant messaging behaviors with traditional SMS. In *Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services* (pp. 352-361).

- **تطبيق Pokes** أو النكزة وهو عبارة عن إشعار يخطر المستخدم بأن أحد الأصدقاء يقوم بالترحيب به[156].

- **تطبيق Photos** أو الصور الذي يُمكن المستخدمين من تحميل الألبومات والصور من أجهزتهم إلى الموقع، يوفر فيسبوك لمستخدميه إمكانية تحميل كم هائل من الصور مقارنة بالمواقع الأخرى. كما أنه يمكن ضبط إعدادات الخصوصية للألبومات الفردية، وبالتالي الحد من مجموعات المستخدمين الذين يمكنهم مشاهدة ألبوم معين. فعلى سبيل المثال، يمكن ضبط إعدادات الخصوصية لألبوم ما بحيث تتيح لأصدقاء المستخدم فقط مشاهدة الألبوم، بينما يمكن ضبط إعدادات الخصوصية في ألبوم آخر على نحو يتيح لجميع مستخدمي فيسبوك مشاهدة هذا الألبوم، كما يمكن هذا التطبيق من تسمية المستخدمين في صورة ما أو إضافة تعليق ما[157].

- **تطبيق Status** أو الحالة التي تتيح للمستخدمين إمكانية إبلاغ أصدقائهم بأماكنهم وما يقومون به من أعمال في الوقت الحالي .

- **تطبيق News Feed** أو التغذية الإخبارية التي تظهر على الصفحة الرئيسية لجميع المستخدمين، حيث تقوم بتمييز بعض البيانات مثل التغييرات التي تحدث في الملف الشخصي، وكذلك الأحداث المرتقبة وأعياد الميلاد الخاصة بأصدقاء المستخدم.

- **تطبيق Gifts** أو الهدايا، التي تتيح للمستخدمين إرسال هدايا افتراضية إلى أصدقائهم تظهر على الملف الشخصي للمستخدم الذي يقوم باستقبال الهدية.

- **تطبيق Marketplace** أو السوق الذي يتيح للمستخدمين نشر إعلانات مبوبة مجانية.

- **تطبيق Events** أو أحداث، الذي يوفر للمستخدمين وسيلة لإبلاغ الأصدقاء عن الأحداث المرتقب وقوعها.

---

(156) Nosko, A., Wood, E., & Molema, S. (2010). All about me: Disclosure in online social networking profiles: The case of FACEBOOK. *Computers in human behavior*, *26*(3), 406-418.

(157) Chen, W., & Fong, S. (2010, July). Social network collaborative filtering framework and online trust factors: A case study on Facebook. In *2010 Fifth international conference on digital information management (ICDIM)* (pp. 266-273). IEEE.

- **تطبيق Video** أو فيديو، الذي يوفر إمكانية تبادل أفلام الفيديو المنزلية بين المستخدمين[158].

نظام تشغيل فيس بوك

قام فيسبوك بطرح نظام تشغيل ــ Facebook Platform ــ عام 2007، ويعتمد ذلك على توفير إطار عمل لمطوري البرامج من أجل إنشاء تطبيقات يمكن أن تتفاعل مع سمات فيسبوك الرئيسة. كما تم تقديم لغة برمجة تستخدم علامات الترميز أُطلق عليها Facebook Markup Language في الوقت نفسه. ويتم استخدام هذه اللغة من أجل تخصيص الشكل العام للتطبيقات التي يقوم المطورون بإنشائها[159].

الواتس اب

هو تطبيق يقوم على استخدام الإنترنت لإرسال الرّسائل النصيّة والصّور والرسائل الصّوتيّة وحتّى مقاطع الفيديو، وتُتاح إمكانيّة استخدامه من خلال تحميله على الأجهزة الخاصّة، سواء الهواتف الذّكية أو أجهزة الحاسب، يمكن استخدام تطبيق الواتساب مع معظم منصات الهواتف الذكية وأنظمة التشغيل، مثل: الآيفون (Iphone)، والأندرويد (Android)، وهواتف بلاك بيري (BlackBerry)، وهواتف ويندوز (Windows Phone) ، وهواتف نوكيا (Nokia phones) .[160]

يتطلّب استخدام الوتس آب أن يمتلك الشّخص جهاز لوحي أو هاتف محمول مع بطاقة (SIM Card) ورقم هاتف، مدعوم بخدمة الإنترنت، وعند تنزيل التطبيق على الهاتف سيتم استخدام رقم الهاتف المحمول كاسم مُستخدم للتطبيق، وبالتّالي سيرتبط استخدام هذا التطبيق بالجهاز الذي تم تنزيل التطبيق عليه.[161]

---

[158] Nosko, A., Wood, E., & Molema, S. (2010). All about me: Disclosure in online social networking profiles: The case of FACEBOOK. *Computers in human behavior*, *26*(3), 406-418.

[159] Chen, W., & Fong, S. (2010, July). op.cit, p. 266-273.

[160] Church, K., & De Oliveira, R. (2013, August). What's up with WhatsApp? Comparing mobile instant messaging behaviors with traditional SMS. In *Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services* (pp. 352-361).

[161] Shahid, S., & Zubairi, N. A. (2016). Comparative Study: An analysis of WhatsApp application and SMS by students & Professionals of Karachi. *Journal of Mass Communication Department, Dept of Mass Communication, University of Karachi*, *14*.

برمجيات الشبكة للفيس بوك والو اتس اب:

يستخدم فيسبوك التكنولوجيا التي تتوافق مع المعايير القياسية لتقسيم الشبكة، حيث يتطلب الوصول عن بُعد إلى أنظمة فيسبوك إجراء اتصالات مشفّرة من خلال استخدام بروتوكولات آمنة. ولحماية البيانات أثناء النقل، يفرض فيسبوك استخدام البروتوكولات المناسبة المصممة لحماية سرية البيانات أثناء نقلها عبر الشبكات العامة. تتمثل هذه البروتوكولات فيما يلي:

- يقدم فيس بوك وواتس اب واجهة آمنة للتصفح عبر بروتوكول نقل النصوص الفائقة الآمن (HTTPs) Hypertext transfert protocol Secure، وهو عبارة عن مزيج من بروتوكول نقل النص الفائق (http) مع خدمة تصميم المواقع (TLS) لتوفير الاتصالات المشفرة (https) وتحديد تأمين شبكة خادم الويب[162].
- بروتوكول (IPv6) Internet Protocol Version 6: يتميز بروتوكول IPv6 والذي يسمى أيضاً IPng (وهذا اختصار لبروتوكول الإنترنت الجيل الثاني Internet Protocol Next Generation) بتوفير مساحة عناوين كبيرة جداً لبروتوكول الإنترنت IP مقارنة بالسابق، حيث أصبح bits128 بدلاً من bits 32، مما أدى لحل مشكلة محدودية العناوين في الإصدار الحالي المطبق في جميع أنحاء العالم، بالإضافة إلى الكثير من المزايا الأخرى. وقد أسهم الإصدار الجديد من بروتوكول الإنترنت في زيادة سهولة وفاعلية التنقل بين الشبكات ودمج إمكانية التشفير والتوثيق داخل البروتوكول نفسه، مع وجود آليات لضمان جودة الخدمة، بالإضافة إلى وجود تقنيات كثيرة للانتقال من الإصدار الرابع إلى الإصدار السادس للبروتوكول.

كما يتميز هذا البروتوكول بالدعم الكامل لنظام الأمان والتشفير IPSec، نظراً لأن الاتصال عبر وسط عام كالإنترنت مثلاً يتطلب خدمات تشفير لحماية البيانات المرسلة من أن تتعرض للكشف أو للتعديل أثناء النقل. بالإضافة إلى أن النظام الجديد يعطي عناوين عالمية فريدة، لذلك فإنه يوفر حماية أمنية متكاملة من نقطة الإرسال إلى نقطة الإستقبال مثل

---

[162] سمية ديمش .(2011). التجارة الإلكترونية حتميتها وواقعها في الجزائر."أطروحة ماجستير"، جامعة منتوري (قسنطينية)، ص 30 .

السـرية Confidentiality وتكامل البيانات Data Integrity و الخصـوصـية Privacy وكل هذا دون التأثير على كفاءة الشبكة[163].

سادساً - الرابطة الأرشيفية

يجب أن تحتوي وثيقة الفيس بوك والواتساب على رابطة أرشيفية، على سبيل المثال، في كثير من الأحيان نجد بعض المنشورات أو الأخبار على فيس بوك مرتبطة بمنشورات أو أخبار قديمة، كتذكر تواريخ أعياد الميلاد، حيث يتم إظهار تاريخ الميلاد بالكامل من خلال التسـلسـل الزمني للأحداث الخاصـة بالمسـتخدم، وقد وُجد أنه من بين خصـائص فيسـبوك خيار يسـمح بتذكر تواريخ أعياد ميلاد المستخدمين الذين تمت إضافتهم إلى قائمة الأصدقاء.

ومن خلال ما سـبق، يتضـح أن المخرجات الناتجة عن مواقع التواصـل الإجتماعي (فيس بوك، واتس اب) قد اسـتوفت جميع متطلبات الوثيقة على النحو المحدد في مشـروع الانتربارس (شكل ثابت ومحتوى مستقر والأشخاص والحدث والسياق والرابطة الأرشيفية)، ولذلك يمكن الحكم على وثائق الفيس بوك والواتس اب أنها وثائق دبلوماتية تستحق النقد من علم الدبلوماتيك لكي يكون لها حجية أمام القضاء.

عناصرالنقد الدبلوماتي لوثيقة الفيس بوك موضوع الجريمة[164]:

تتلخص وقائع هذه القضية في قيام أحد الأشخاص بسرقة صفحة حساب الفيس بوك الخاص بالمجني عليها، والتحصل منه على صور شخصية لها وإرسال رسائل لأصدقائها وأقاربها تتضمن عبارات سب وقذف في حقهم وإرسال صور شخصية للمجني عليها تتضمن الإساءة لسمعتها مما ألحق بها أضراراً جسيمة.

- السياق[165]

1 - سياق المصدر

تبدأ عملية الإثبات وفقاً للإثبات الجنائي والدبلوماتيك الرقمي بفحص مصـدر الوثيقة، وذلك بالبحث عن من هو الشخص المسؤول عن سرقة حساب الفيس بوك للمجني عليها، وإرسال الرسائل لأصدقائها، ثم التعرف على المصدر وتحديده من خلال فحص حساب

---

[163] Chen, W., & Fong, S. (2010, July). op.cit, p. 266-273.

[164] وثائق قضية جنحة رقم 307 لسنة 2017 جنح اقتصادية القاهرة.

[165] قضية جنحة رقم 307 لسنة 2017 جنح اقتصادية القاهرة.

المجني عليها والمُسمى (----)، والذي تبين من خلاله أن ذلك الحساب قد استخدم الرقم التعريفي IP: 41.47.218.15 بتاريخ 2016/5/11 الساعة 23:58 مساءً بتوقيت القاهرة، وبتتبع الرقم التعريفي المشار إليه على شبكة الإنترنت، تبين أنه صادر من جهازADSL مرتبط برقم تليفون أرضي (-------)، مسجل باسم المتهم – وعنوانه (------)[166].

ويعتبر ما قام به قسم المعلومات الجنائية بالإدارة العامة لتكنولوجيا المعلومات مطابقاً لمنهج الدبلوماتيك الرقمي، حيث يبدأ الفحص الدبلوماتي بفحص مصدر الوثيقة من خلال تحليل العناصر الخارجية والداخلية لوثيقة الفيس بوك للتعرف على الشخص الذي قام بسرقة حساب الفيس بوك الخاص بالمجني عليها، فمن خلال تحليل العناصر الخارجية والداخلية يمكن تحديد الجاني والمجني عليه والأشخاص الذين تم إرسال الرسائل إليهم وتواريخ الإرسال والحدث الذي شاركت فيه الوثيقة، إلا أنه وفقاً للدبلوماتيك الرقمي كان يجب فحص نظام تشغيل الفيس بوك والبيانات الواصفة له (الميتاداتا) وفحص مفاتيح التسجيل واستقصاء أنشطة الفيس بوك من خلال أدلة التطبيقات وتحديد أدوات القرصنة التي استخدمت في سرقة الحساب..

والجدول رقم (12) يوضح ميتاداتا الهوية لوثيقة الفيس بوك:

عناصر الميتاداتا	التطبيق
أسماء الأشخاص المسؤولين عن الحدث	المسئول (المرسل): صاحب الرقم التعريفي IP: 41.47.218.15 (المتهم أو الجاني) لحساب الفيس بوك، المُسمى (-----)، حيث تبدأ صفحة الفيس بوك باسم الحساب مرفق بها صورة الملف الشخصي للمستخدم. المستلمين: حسابات الفيس بوك الخاصة بأصدقاء المجني عليها، في الشكل الموضح تظهر سمة لوحة الحائط (WALL) وهي عبارة عن مساحة مخصصة في صفحة الملف الشخصي لأي مستخدم، متاحة لجميع الأصدقاء، وبإمكان أي مستخدم أن يدخلها ويتصفح ما بها من معلومات شخصية.

[166] انظر الملحق السابع من رسالة حسناء علي علي. (2022)، (تقرير الفحص الفني لقضية جنحة رقم 307 لسنة 2017 جنح اقتصادية القاهرة)، ص 347 – 348.

عناصر الميتاداتا	التطبيق
التاريخ ووقت الإنشاء	2016/5/11- الساعة 23:58 مساءً بتوقيت القاهرة، وهو مدون باللغة الإنجليزية أسفل الرسالة
الموضوع الذي شاركت فيه	حصول الجاني على توقيع الوسيط الإلكتروني (صفحة الفيس بوك الخاص بالمجني عليها) وقيامه بإرسال رسائل لأصدقائها وأقاربها تتضمن عبارات سب وقذف في حقهم وإرسال صور شخصية للمجني عليها تتضمن الإساءة لسمعتها مما ألحق بها أضراراً جسيمة.
العرض الرقمي	خصائص العرض - رسائل فيس بوك عبارة عن نصوص مكتوبة وتحوي صورة ضوئية للمجني عليها، مضافاً إليها بعض التعليقات ولا تحوي أي تسجيلات صوتية. - يختار صاحب حساب الفيس بوك نظام الألوان الخاص بواجهة الصفحة، كما يمكن للمستخدم التحكم في تنسيق النصوص والخطوط في منشوراته من خلال ضبط الإعدادات.
التوقيع الإلكتروني	- لا يوجد توقيع إلكتروني، وإنما يُسمى بتوقيع الوسيط الإلكتروني (فيس بوك)، وذلك بإدخال المستخدم لكلمة المرور التي تم التسجيل من خلالها إلى فيس بوك لحماية الحساب.

2- سياق الإجراءات

يمكن تقسيم التحليل الدبلوماتي للمراحل الإجرائية في إنشاء الدليل الجنائي على النحو التالي:

أ) المبادرة (الإعداد لعملية التحقيق الجنائي):

تبدأ مرحلة المبادرة وفقاً للإثبات الجنائي، بإجراءات إبلاغ المجني عليها بتضررها من قيام مجهول بسرقة حساب الفيس بوك الخاص بها والمُسمى (-----) على موقع التواصل الاجتماعي فيس بوك بشبكة المعلومات الدولية (الإنترنت).

ب) التحقيق (جمع الوثائق (الأدلة) الرقمية الصحيحة):

تبدأ مرحلة التحقيق وفقاً للإثبات الجنائي، بفحص البلاغ المُقدم من قبل المجني عليها وإجراء التحريات اللازمة للتحقيق، وذلك عن طريق تتبع حساب الشاكيه، والذي تبين من

خلاله قيام أحد الأشخاص بسرقة حساب المجني عليها والمُسمى (---) والتحصل منه على صور شخصية لها وإرسال رسائل لأصدقائها تتضمن إساءة لها، وبسؤال الشاكية (المجني عليها) عن علاقتها بالجاني قررت أن الجاني هو والد خطيبة شقيقها وأنه يوجد خلافات سابقة مع نجلته المدعوة (-).

ج) التشـــاور(فحص المواد الرقمية): تتضـــمن مرحلة التشـــاور التحقق من جميع الوثائق المقدمة، مع الإستعانة بتقرير الفحص الفني بشأن الأدلة المقدمة ضد المتهم، مرفق بالتقرير لقطات مطبوعة من تلك الرسائل.

تبدأ مرحلة التشـاور وفقاً للإثبات الجنائي، بفحص الرسـائل المرسـلة إلى أصـدقاء المجني عليها وفحص حساب المجني عليها والمُسمى (-----)، كما ذكرنا سابقاً في سياق المصدر.

د) التداول (مرحلة تدوين النتائج وإعداد التقرير):

تتضـمن هذه المرحلة وفقاً للإثبات الجنائي، إعداد التقارير عن الأنشـطة والفحوص التي تمت، وتدوين النتائج، نظراً للثابت من أقوال المجني عليها بمحضـر جمع الاسـتدلالات، وتقرير الفحص الفني المؤرخ 2016/7/17 والمُحرر بمعرفة النقيب مهندس/ أيمن فكري (الضابط بقسم المساعدات الفنية)، وتتمثل هذه المرحلة في إعداد محاضر التحريات وتقرير الفحص الفني وتقديمها للنيابة العامة.

هـ) مر اقبة التداول (تقديم حزمة الأدلة):

تتضـمن هذه المرحلة وفقاً للإثبات الجنائي، قيام النيابة العامة بتقديم المتهم للمحاكمة وتكليفه بالحضور، إلا أن المتهم لم يمثل أمام القضاء رغم إعلانه قانوناً.

و) التنفيذ(إدارة مواد القضية):

تُشـير هذه المرحلة إلى التأكد من توافر الركن المادي والمعنوي لارتكاب الجريمة، تتحقق أركان الجريمة في قيام المتهم بالاستيلاء على الحساب المُسمى(------) على موقع التواصل الاجتماعي فيس بوك بشبكة المعلومات الدولية (الإنترنت) وقيامه بإرسال رسائل لأصدقائها وأقاربها تتضمن عبارات سب وقذف في حقهم وإرسال صور جنسية للتشهير بها وإساءة سمعتها وبتتبع الحساب تبين أنه مرتبط برقم تليفون أرضي مسجل باسم المتهم وعنوانه، وعليه فقد اسـتقر في يقين المحكمة ووجدانها اقتراف المتهم لكافة الجرائم المسـندة إليه بالأوراق بكافة أركانها القانونية، حيث تتجلى جريمة إزعاج المجني عليها وذلك بإسـاءة اسـتعمال أجهزة

الاتصـــالات كما أن المتهم توصـــل بغير وجه حق للحصـــول على الوســـيط الإلكتروني المملوك للمجني عليها الأمر الذي ترى معه المحكمة عقاب المتهم وفقاً لأحكام المادة (23/هـــ) من قانون التوقيع الإلكتروني المصري، وعملاً بنص المادة 2/304 من قانون الإجراءات الجنائية.

كما تتضمن مرحلة التنفيذ وثيقة النطق بالحكم أول درجة ضد المتهم. وقد ترتب على هذه المرحلة عدة إجراءات فرعية، حيث طعن المتهم على هذا الحكم بطريق المعارضـــة بموجب تقرير تم إيداعه في قلم كتاب المحكمة مثبت به تاريخ الجلســـة، ولما كانت أوراق الجُنحة قد خلت مما يُفيد إعلان الحُكم لشخص المتهم المُعارض أو تاريخ علمه بحصول ذلك الإعلان، الأمر الذي تكون معه المعارضـة قد أُقيمت بالأوضـاع والإجراءات الصـحيحة المنصـوص عليها قانوناً ومن ثم تكون مقبولة شـكلاً على نحو ما سـيرد بالمنطوق. أما عن موضـوع المعارضـة فإنه من المسـتقر عليه أنَ لمحكمة الموضـوع الحق في أن تسـتمد اقتناعها من أي دليل تطمئن إليه مادام له مأخذه من الأوراق، وحيث أنه قد اســـتقر في يقين المحكمة ووجدانها اقتراف المتهم المعارض لكافة الجرائم المســـندة إليه، ولما كان الحُكم المعارض قد التزم هذا النظر وقضـى بإدانة المُتهم فإنه يكون قد طبق القانون تطبيقاً صـحيحاً ومن ثم فإن هذه المحكمة تعتنق أسـباب ذلك الحُكم وتأخذ بها مُكملة لأسباب حكمها، إلا أنه بقيام المجني عليها بتنازلها عن شكواها وبالنظر لظروف الواقعة وملابســاتها واطمئنان المحكمة إلى أن المُتهم المُعارض لن يعود لمثل ذلك الفعل مســـتقبلاً، وطبقاً للمادتين (55)، (56) من قانون العقوبات المصـــري فالمحكمة توقف تنفيذ العقوبة المقضي بها على نحو ما سيرد بالمنطوق[167].

ونظراً لأن النيابة العامة لم ترتض هذا القضـــاء فقد طعنت عليه بطريق الاســـتئناف للخطأ في تطبيق القانون بموجب تقرير اســـتئناف مؤرخ 2017/5/30 وقدمت مذكرة بأســـباب استئنافها طلبت في ختامها الحكم أولاً بقبول الاستئناف شكلاً، ثانياً وفي الموضوع بإلغاء الحُكم المُستأنف وتطبيق صحيح القانون تأسيساً على إغفال محكمة أول درجة الحُكم بالنشر طبقاً لنص المادة 23 من قانون تنظيم التوقيع الإلكتروني المصري.

ولما كان الاستئناف مستوفياً لأوضاعه الشكلية المقررة قانوناً فقد تم قبوله شكلاً.

---

[167] انظر الملحق الثامن من رسالة حسناء علي علي. (2022)، (وثائق المعارضة رقم 307 لسنة 2017 جنح اقتصادية القاهرة)، ص349 - 352.

أما عن موضوع الاستئناف، لما كانت محكمة أول درجة قد قضت بإدانة المستأنف ضده وساقت للتدليل على ثبوت الاتهامات المنسوبة إليه أسباباً سائغة لها أصلها الثابت بالأوراق ومستمدة من أقوال المجني عليها بمحضر جمع الاستدلالات، وتقرير الفحص الفني المؤرخ 2016/7/17 والذي أثبت ما نُسب للمتهم من جرائم، الأمر الذي استقر معه في يقين المحكمة ووجدانها اقتراف المتهم لكافة الجرائم المسندة إليه بالأوراق بكافة أركانها القانونية، إلا أنَ محكمة أول درجة قد أغفلت القضاء بعقوبة نشر الحُكم على شبكة المعلومات الإلكترونية المفتوحة على نفقة المحكوم عليه – وهي عقوبة تكميلية وجوبية يجب القضاء بها عند الإدانة – الأمر الذي يكون معه استئناف النيابة العامة قد جاء على سند صحيح من الواقع والقانون وتقضي المحكمة بتعديل الحُكم المستأنف بإضافة تلك العقوبة والتأييد فيما عدا ذلك على نحو ما سيرد بالمنطوق[168].

3 - السياق القانوني والإداري:

يظهر السياق القانوني في الحكم الصادر من المحكمة ضد المتهم، حيث قضت محكمة أول درجة بحبس المتهم لمدة ثلاثة أشهر وكفالة قدرها ألف جنيه مع إيقاف تنفيذ عقوبة الحبس مؤقتاً وتغريمه مبلغ وقدره ثلاثين ألف جنيه ونشر ملخص الحكم في جريدة الأهرام وجريدة الأخبار على نفقة المتهم والزمته المصاريف الجنائية[169].

وفقاً للحكم الصادر فقد تمت معاقبة المتهم وفقاً لأحكام المادة 2/76 من قانون تنظيم الإتصالات رقم 10 لسنة 2003، والمادتين 1/23 فقرة (هـ)، (4) من القانون رقم 15 لسنة 2004 بشأن تنظيم التوقيع الإلكتروني المصري، والمادة (313) من قانون الإجراءات الجنائية.

- الوسيط

جهاز الراوتر ADSL والمرتبط بخط تليفون أرضي.

---

[168] انظر الملحق التاسع من رسالة حسناء علي علي. (2022)، (وثائق قضية جنحة رقم 484 لسنة 2017 جنح مستأنف ورقم 307 لسنة 2017 جنح اقتصادية القاهرة)، ص 353 - 355.

[169] وثائق قضية جنحة رقم 307 لسنة 2017 جنح اقتصادية القاهرة.

والجدول رقم (13) يوضح مدى مطابقة الفحص الجنائي الرقمي لمنهج علم الدبلوماتيك الرقمي في جريمة سرقة حساب الفيس بوك المُسمى (--------):

وجه المقارنة	الفحص الجنائي الرقمي	عناصرالنقد (الفحص) الدبلوماتي الرقمي	مطابق	غير مطابق
الخصائص الخارجية	فحص عنوان IP لحساب الفيس بوك المُسمى (-----)، وتتبع الرقم التعريفيIP	خصائص العرض	مطابق	
الخصائص الداخلية	فحص محتوى رسائل الفيس بوك	الخصائص الداخلية	مطابق	غير مطابق
	تحديد عنوان IP الخاص بكل رسالة وتحديد المرسل	المسؤول أو المرسل(الجاني)	مطابق	
	تحديد المرسل إليه	أصدقاء المجني عليها	مطابق	
	تحديد تاريخ الإرسال	التاريخ الزماني	مطابق	
	تحديد الموقع الجغرافي للجهاز الذي حدثت العملية من خلاله	التاريخ المكاني	مطابق	
	تحديد الموضوع الذي شاركت فيه الوثيقة	وصف الحدث	مطابق	
الوسيط	فحص جهاز الراوتر ADSL	الوسيط	مطابق	
السياق	تتبع الرقم التعريفيIP	سياق المصدر	مطابق	
	تحديد إجراءات الإثبات الجنائي	سياق الإجراءات	مطابق	
	تحديد الإطار القانوني الذي تتم فيه الدعوى الجنائية	السياق القانوني	مطابق	

الجريمة الخامسة: رسالة و اتساب تتضمن عبارات سب وتهديد للمجني عليها وأسرتها[170]

تتلخص وقائع هذه القضـــية في قيام الجاني بتهديد المجني عليها، كتابة بنســـبة أمور مخدشـة بالشـرف، وذلك بإرسـال رسـائل لها عبر تطبيق واتسـاب تتضـمن عبارات سـب وتهديد للمجني عليها وأسرتها.

النقد الدبلوماتي لوثيقة الو اتساب Whatsapp كوثيقة تفاعلية غير ديناميكية

أولاً- السياق

1 - سياق المصدر

تبدأ عملية الإثبات وفقاً للإثبات الجنائي بفحص مصـدر الوثيقة، وذلك بالبحث عن من هو الشخص المسؤول عن إرسال الرسالة إلى المجني عليها، ثم التعرف على مصدر الرسالة من خلال الإستعلام عن بيانات خط الهاتف المحمول رقم (--------) من شركة أورنج والذي تبين أن بياناته مسجلة باسم/ --------، وعنوانه ---------- حدائق القبة القاهرة.

ويُعتبر ما قامت به إدارة مكافحة جرائم الحاسـبات وشـبكات المعلومات مطابقاً لمنهج علم الدبلوماتيك الرقمي، حيث يبدأ النقد الدبلوماتي بفحص مصـدر الوثيقة من خلال تحليل العناصـر الخارجية والداخلية لوثيقة الواتسـاب للتعرف على الشـخص المسـؤول عن إرسـال الرسـالة إلى المجني عليها، فمن خلال تحليل العناصـر الخارجية والداخلية يمكن تحديد الجاني والمجني عليها وتواريخ الإرسـال والحدث الذي شـاركت فيه الوثيقة. وفيما يلي سـوف يتم تحليل العناصر الخارجية والداخلية لوثيقة الواتساب وفقاً لمنهج علم الدبلوماتيك الرقمي:

أ- العناصر الخارجية:

- **خصائص العرض**
- رسـالة واتسـاب عبارة عن نص مكتوب وتحوي صـورة ضـوئية للمجني عليه ومرفق بها إثنين من التسجيلات الصوتية للجاني.
- لا يوجد توقيع إلكتروني، وإنما يختار صـاحب الهاتف تنسـيق رسـالة الواتسـاب من حيث حجم الخط ولونه وخلفية الشـاشـة، واختيار مظهر الشـاشـة وإعدادات الدردشـة من نقل وأرشفة ومسح وحذف المحتوى.

[170] قضية جنحة رقم 271 لسنة 2019 جنح اقتصادية القاهرة.

ب - العناصر الداخلية:

المسئول (المرسل): مستخدم رقم الهاتف المحمول، وهو مدون باللغة الإنجليزية في أعلى نص الرسالة، حيث بدأت رسالة الواتساب برقم التليفون الخاص بالجاني، ذلك لأنه غير مسجل ضمن قائمة اتصال المرسل إليه، تلاها صورة المجني عليها.

المرسل إليه (الموجهة إليه الرسالة): المجني عليها، حيث يتم عرض جهة الإتصال (اسم ورقم المرسل إليه) ضمن قائمة الإعدادات.

الدولة التابع لها: مصر.

تاريخ الإرسال: لم يظهر التاريخ في الرسالة الأولى وإنما ظهر توقيت الرسالة أسفل النص مدون باللغة الإنجليزية وهو 4:33 صباحاً، أما التسجيلات الصوتية فقد ذُكر في أعلاها التاريخ مدون باللغة الإنجليزية وهو 23 أكتوبر2018، كما ذُكر توقيت ومدة التسجيل الصوتي أسفل التسجيل باللغة الإنجليزية، وهو كالتالي: التسجيل الأول توقيت 3:06 صباحاً ومدته 38 ثانية أما التسجيل الثاني توقيت 3:06 صباحاً ومدته 58 ثانية.

الموضوع: رسائل واتساب واردة للمجني عليها.

وصف الحدث: رسالة واتساب تتضمن عبارات سب وتهديد للمجني عليها وأسرتها[171].

2 - سياق الإجراءات[172]

يمكن تقسيم التحليل الدبلوماتي للمراحل الإجرائية في إنشاء الدليل الجنائي على النحو التالي:

أ) المبادرة (الإعداد لعملية التحقيق الجنائي):

تبدأ مرحلة المبادرة بمجرد إبلاغ المجني عليها بإرسال المتهم رسائل لها عبر تطبيق الواتساب من هاتفه المحمول تتضمن عبارات سب وتهديد لها ولأسرتها وقد قدمت المجني عليها هاتفها المحمول لمناظرة تلك الرسائل وصور ملطقته مطبوعة لتلك الرسائل.

---

[171] انظر الملحق العاشر من رسالة حسناء علي علي. (2022)، (صورة ضوئية لوثيقة الواتساب لقضية جنحة رقم 271 لسنة 2019 جنح اقتصادية القاهرة)، ص 356 - 359.

[172] وثائق قضية جنحة رقم 271 لسنة 2019 جنح اقتصادية القاهرة.

ب) التحقيق (جمع الوثائق (الأدلة) الرقمية الصحيحة):

تبدأ مرحلة التحقيق بالإســتعلام عن بيانات خط الهاتف المحمول رقم (--------) من شركة أورنج خلال الفترة من 2018/11/27 حتى 2018/11/29، والذي تبين أن بياناته مسجلة باسم/ المتهم وعنوانه.

ج) التشاور(فحص المواد الرقمية):

تتضـمن مرحلة التشـاور فحص مصـدر وثيقة الواتسـاب، وذلك بالبحث عن من هو الشـخص المسـؤول عن إرسـال الرسـالة إلى المجني عليها، ثم التعرف على مصـدر الرسـالة كما ذكرنا سابقاً في سياق المصدر.

د) التداول (مرحلة تدوين النتائج وإعداد التقرير):

تتضــمن هذه المرحلة وفقاً للإثبات الجنائي إعداد التقارير عن الأنشــطة والفحوص التي تمت، وتدوين النتائج، وتقديمها للنيابة العامة.

هـ) مر اقبة التداول (تقديم حزمة الأدلة):

تتضــمن هذه المرحلة وفقاً للإثبات الجنائي، تقديم كل الوثائق والتقارير إلى الفريق القانوني لإرفاقها مع المواد التي سوف يتم تقديمها إلى المحكمة.

و) التنفيذ (إدارة مواد القضية):

تُشــير هذه المرحلة إلى التأكد من توافر الركن المادي والمعنوي لارتكاب الجريمة، وتحديد ما إذا كان الفعل المرتكب يُشكل إزعاجاً أو مضايقة للمتلقي من عدمه، فضلاً عن كون المتهم لم ينفِ التهمة عن نفســه أو يقدم دفعاً يجعل المحكمة تتشـكك في صحة الواقعة الأمر الذي تتوافر معه أركان جريمة الإزعاج باســتخدام وســائل الاتصــالات في حق المتهم، إلا أنه وبثبوت تلك الجريمة في حق المتهم فقد ثبت في حقه باقي الجرائم المســندة إليه من قبل النيابة العامة حسبما جاء بمواد الاتهام مما يكون قد شكل الفعل الإجرامي أكثر من جريمة بما يتحقق معه التعدد المعنوي للفعل الواحد، وهو ما تقضــي معه المحكمة بمعاقبته وفقاً لأحكام المادة (32) من قانون العقوبات ومعاقبته بعقوبة الجريمة الأشــد المؤثمة بالمادة 2/76 من القانون رقم 10 لسنة 2003 بشأن تنظيم الاتصالات، وبنص الفقرة الأخيرة من المادة (304) من قانون الإجراءات الجنائية. كما تتضمن مرحلة التنفيذ وثيقة النطق بالحكم ضد المتهم.

3 - السياق القانوني والإداري:

يظهر السياق القانوني في الحكم الصادر من المحكمة ضد المتهم، والذي ينص على:

حبس المتهم لمدة شـــهرين مع الشـــغل وكفالة قدرها ألف جنيه مع إيقاف تنفيذ عقوبة الحبس مؤقتاً وتغريمه مبلغ وقدره عشرين ألف جنيه والمصاريف.

وفقاً للحكم الصـــادر فقد تمت معاقبة المتهم وفقاً لأحكام المادة 2/76 من قانون تنظيم الإتصالات رقم 10 لسنة 2003، المادة (32) من قانون العقوبات، وبنص الفقرة الأخيرة من المادة (304) من قانون الإجراءات الجنائية، وبالنسـبة للمصـروفات الجنائية فإن المحكمة تلزم بها المتهم عملاً بنص المادة 313 من قانون الإجراءات الجنائية.

- الوسيط

شريحة الهاتف المحمول SIMالمسجلة باسم المجني عليها، التي يتم ضبطها بالمعلومات الأساسية من أجل تحديد هوية الهاتف المحمول حتى يستطيع استقبال المكالمات والرسائل.

والجدول رقم (14) يوضح مدى مطابقة الفحص الجنائي الرقمي لمنهج علم الدبلوماتيك الرقمي في جريمة وثيقة الو اتساب:

وجه المقارنة	الفحص الجنائي الرقمي	عناصر النقد (الفحص) الدبلوماتي الرقمي	مطابق	غير مطابق
الخصائص الداخلية	تحديد رقم التليفون المرسل للرساله	المسؤول أو المرسل(الجاني)	مطابق	
	تحديد المرسل إليه	المجني عليها	مطابق	
	تحديد تاريخ الإرسال	التاريخ الزماني	مطابق	
	تحديد الموقع الجغرافي لمرسل الرسالة	التاريخ المكاني	مطابق	
	تحديد الموضوع الذي شاركت فيه الوثيقة	وصف الحدث	مطابق	

وجه المقارنة	الفحص الجنائي الرقمي	عناصر النقد (الفحص) الدبلوماتي الرقمي	مطابق	غير مطابق
الوسيط	فحص شريحة الهاتف المحمول	الوسيط	مطابق	
السياق	الاستعلام عن بيانات خط الهاتف المحمول	سياق المصدر	مطابق	
	تحديد إجراءات الإثبات الجنائي	سياق الإجراءات	مطابق	
	تحديد الإطار القانوني الذي تتم فيه الدعوى الجنائية	السياق القانوني	مطابق	

الخاتمة

من خلال التطبيق العملي لمنهج علم الوثائق (الدبلوماتيك) الرقمي على نماذج الوثائق (الأدلة الجنائية الرقمية) للجرائم المعلوماتية، أوضحت الدراسة وجود تطابق بين منهج علم الوثائق (الدبلوماتيك) الرقمي وعلم الإثبات الجنائي الرقمي، حيث خلصت الدراسة إلى أنه:

1 - يبدأ النقد (الفحص) الدبلوماتي للوثائق (الأدلة) الجنائية الرقمية بنقد المصدر أو فحص المصدر وكذلك في الإثبات الجنائي تبدأ عملية الإثبات بفحص مصدر الوثيقة الرقمية.

2 – لا يمكن تطبيق منهج علم الدبلوماتيك الرقمي بشكلٍ نظامي على الوثائق أو الأدلة الجنائية الرقمية لأن كل دليل له طبيعه خاصة تميزه عن غيره فبعض الأدلة تحتاج إلى تحليل عناصر الشكل الخارجي والداخلي للوصول إلى الجاني والبعض الآخر يحتاج إلى استخراج عناصر ميتاداتا الهوية والتكامل.

3 – يتطابق التحليل الدبلوماتي لإجراءات الحصول على الدليل الجنائي الرقمي مع الأنشطة الإجرائية الستة التي حددها نموذج الإثبات الجنائي الرقميDRF.

4 – يشرح الفحص الفني للوثائق (الأدلة) الرقمية السياق التقني للبيئة التي أنشأت هذه الوثائق (الأدوات والكيفية التي ارتكبت بها الجريمة).

وقد توصلت هذه الدراسة إلى عدة نتائج مهمة وهي:

1 - يحتاج الوثائقي والأرشيفي إلى دراسة علوم الحاسبات حتى يتمكن من معرفة الظروف التقنية للوثيقة الرقمية والتي تساعده في تقييم صحتها، الأمر الذي يجعله مؤهلاً للعمل في مكاتب التحقيق الجنائي الرقمي.

2 - يجب أن يكون الوثائقي (الدبلوماتي) والأرشيفي ملماً بمجموعة متنوعة من المهارات التي تؤهله للعمل في مكاتب التحقيق الجنائي الرقمي، وتتمثل هذه المهارات فيما يلي:

- القدرة على فهم الوثائق التي تم إنشاؤها وحفظها في البيئة الرقمية.
- القدرة على تحديد هوية الوثائق من بين الكيانات الرقمية الأخرى الموجودة معها في نفس البيئة.
- القدرة على تحليل الوثيقة الرقمية الظاهرة إلى مكوناتها الرقمية.
- القدرة على فهم إجراءات التوثيق التقني وعلاقته بوسائل التوثيق الأرشيفي.

3 - أصبح للأرشيفي دور كبير في عملية الإثبات الجنائي عند تحريز الوثائق أو الأدلة، حيث يتولى الأرشيفي مسئولية إجراء الضبط الفكري والإداري للوثائق (الأدلة) من خلال الوصف الأرشيفي للأدلة، وبذلك يصبح الأرشيفي مسؤولاً عن الوثائق (الأدلة) ويستطيع التحدث عن هويتها وسلامتها، فهو بمثابة وصي مؤتمن على هذه الوثائق (الأدلة) ويمنح الجدارة بالثقة للوثائق (الأدلة) بموجب هذه المسؤولية.

4 - تكمن أوجه التشابه بين مجالي الأرشيف والإثبات الجنائي في أن كل وظيفة منهما لها مهمة الحصول على "أدلة نزيهة" فكلاهما وظيفته التزويد أو الإضافة وحفظ وترتيب وإتاحة "الأدلة الموضوعية", وتوضيح معنى هذه الأدلة من خلال "معارفه وطرقه التي تميزه" .

5 - إن قيمة النموذج المقترح لمشروع الإثبات الجنائي للوثائق الرقمية DRF, تكمن في مشاركة المعرفة بين التخصصات العلمية (الإثبات الجنائي الرقمي والدبلوماتيك الرقمي وعلم الأرشيف، وقانون الأدلة), مما سوف يثري فهم وتفسير كل مهنة للوثائق (الأدلة) الرقمية.

6 - تناول المشـــروع البحثي للإثبات الجنائي للوثائق الرقمية (DRF) بعض التحديات التي تطرحها التكنولوجيا الرقمية لإدارة الوثائق والأرشـــيف والمهن القانونية، ومن بين هذه التحديات؛ تحديد الوثائق في الأنظمة الرقمية المعقدة وتحديد أصالتها.

7 - اعتمد المشـــروع البحثي للإثبات الجنائي للوثائق الرقمية (DRF) على منهجية الإثبات الجنائي الرقمي والدبلوماتيك الرقمي وعلم الأرشـــيف، ومبادئ قانون الأدلة، وأســـفر عن التخصص الجديد المقترح، وهو الإثبات الجنائي للوثائق الرقمية DRF.

8 - يعتبر إنشـــاء هذا النموذج العام لعملية الإثبات الجنائي للوثائق الرقمية خطوة أولى على طريق تطوير مفهوم علمي لكيفية تكامل الممارســـات الدبلوماتية الأرشـــيفية مع ممارسات الإثبات الجنائي الرقمي للتحقق من الوثائق وتقييمها لأغراض الحصول على الأدلة.

وبعد عرض النتائج توصي الدراسة بالتوصيات التالية:

1 - نشـــر الوعي المجتمعي بأهمية الدور الجديد للوثائقيين في مجال الإثبات الجنائي الرقمي، حيث أصـــبح مســـئولو الفحص الجنائي للوثائق، يلجأون إلى علم الوثائق (الدبلوماتيك) ويستخدمون منهجيته لإثبات صحة الوثائق أو زيفها.

2 - ضرورة إعداد التدريب المناسب للوثائقيين في مجال الإثبات الجنائي، بما يتناسب مع دورهم الجديد في إثبات صحة الوثائق أو زيفها، وبالتالي تتغير صـورة الوثائقي في ذهن المجتمع، ويُصبح مؤهلاً للعمل في مكاتب التحقيق الجنائي.

3 - ضـرورة إعداد التدريب المناسـب للأرشـيفيين في مجال الإثبات الجنائي، بما يتناسـب مع دورهم الجديد في التصـديق على هوية وسـلامة المواد التي تقع تحت مسـؤوليتهم، حيث يُنظر إليهم باعتبارهم خبراء في وصف وتفسير تلك المواد.

4 - ضرورة تطوير المناهج والمفاهيم التي ستتيح للمتخصصين في علوم الوثائق والأرشيف والمعلومات والقانون والإثبات الجنائي الرقمي التعرف على الوثائق في مختلف البيئات الرقمية، وتحديد مدى صـحتها ومصـداقيتها، وذلك من خلال دمج مفاهيم ومناهج جميع العلوم سـابقة الذكر مما يُسـفر عن تطوير وتنظيم مجال علمي جديد متعدد التخصـصـات يُسـمى "الإثبات الجنائي للوثائق الرقمية (DRF) Digital Records Forensics".

5 - نشـــر الوعي المجتمعي بالمخاطر الإجتماعية والســـياســـية والإقتصـــادية والثقافية النـاجمـة عن الإســـتخـدام غير الآمن للإنترنـت، وتبني اســـتراتيجيـة قوميـة للتوعيـة والتثقيف بخطورة الجرائم المعلوماتية والحد من آثارها.

6 - تفعيل التعاون الدولي والإقليمي في مجال الأمن الإلكتروني.

7 - ضرورة تخصيص عدد من المنح التدريبية التخصصية التي يوفرها المتخصصون في مجال الأمن الإلكتروني.

8 - إعداد برامج دراسية لتخصص الوثائق والأرشيف في مجال الأمن الإلكتروني في مرحلة التعليم الجامعي.

المصادروالمراجع

أولاً: المراجع العربية:

1- **إبراهيم الدســـوقي أبوالليل** . (2005). التوقيع الإلكتروني ومدى حجيته في الإثبات.مجلة الحقوق ومجلس النشر العلمي، 3(29).

2- **أحمـد الســـيـد الصـــاوي.** (2010). المحـاكم الاقتصـــاديـة. مجلـة البحوث القـانونيـة والاقتصادية، (1).

3- **أحمد فتحي ســرور**. (1985). الوســيط في قانون الإجراءات الجنائية. القاهرة: دار النهضــة العربية.

4- **أحمد محمد الشامى.** مصطلحات المكتبات والمعلومات والأرشيف . متاح على الرابط التالى : https:// www.elshami.com/Terms/C/htm

5- **أحمد محمود موافي.** (2010). الموسوعة الشاملة في المحاكم الاقتصادية. ط2. القاهرة: دار الحقوق.

6- **أحمد هاني مختار.**(2006). موسـوعة المحاكم الاقتصـادية: الجرائم وعقوباتها. القاهرة: دار النهضة العربية.

7- **أسـامه محمد عطية خميس.** (2013). الكيانات الرقمية (المحتوى الرقمي) في المسـتودعات الرقمية على شـبكة الإنترنت : المفهوم . البرمجيات . البناء . الإيداع الرقمي . الجزء الأول . القاهرة : الشركة العربية المتحدة للتسويق والتوريدات.

8- **إســلام جمال صــابر إبراهيم.**(2016). خدمات التوقيع الإلكترونى فى توثيق المعاملات الإلكترونية الجارية : دراسة لعينة من المؤسسات المصرية. "أطروحة ماجستير"، جامعة القاهرة.

9- **إســلام جمال صــابر إبراهيم.**(2021). الحوســبة الســحابية للوثائق الإلكترونية من واقع مشروع انتربارس (Interpares). "أطروحة دكتوراه"، جامعة القاهرة.

10- **أشــرف توفيق شــمس الدين. (**2003**) .** الحمايه الجنائيه للمســتند الإلكتروني: " دراســه مقارنه". دراســه مقدمه إلى مؤتمر الأعمال المصــرفيه الإلكترونية بين الشــريعه والقانون, مجموعة أعمال المؤتمر, المجلد الثانى, الإمارات العربيه المتحده.

11- **أشــرف محمد عبدالمحســن الشــريف.** (2008). تصــنيف وفهرســة الوثائق الإلكترونية في الإدارات الحكومية. مجلة العربية 3000، 8 (33).

12- **أماني محمد عبد العزيز** . (2017). الميتاداتا ودورها في العمل الأرشــيفي: معيار وصــف الجهات الأرشيفية (EAG) نموذجاً. هرمس. مركز اللغات والترجمة جامعة القاهرة، (19).

13- **أيمن رمضــان الزيني.** (2015). المحاكم الإقتصــادية ودورها في تشــجيع الاســتثمار. دراســة مقــدمــة إلى مؤتمر القــانون والاســــتثمــار ، جــامعــة طنطــا. متــاح على الرابط التــالي: https://law.tanta.edu.eg/files/pdf

14- **أيمن ســـعد ســـليم .** (2004). التوقيع الإلكتروني: دراســـة مقارنة. القاهرة: دار النهضـــة العربية.

15- **ثروت عبد الحميد** . (2007). التوقيع الإلكتروني . الأسكندرية : دار الجامعة الجديدة .

16- **ثناء أحمد محمد المغربي.**(2003).الوجهة القانونية لبطاقات الائتمان. دراســـه مقدمه إلى مؤتمر الأعمال المصـــرفيه الإلكترونيه بين الشـــريعه والقانون, مجموعة أعمال المؤتمر, المجلد الخامس, الإمارات العربيه المتحده .

17- **ثنيان ناصـــر آل ثنيان.** (2012). إثبات الجريمة الإلكترونية: دراســـة تأصـــيلية تطبيقية. "أطروحة ماجستير"، جامعة نايف العربية للعلوم الأمنية.

18- **جمال الخولي.** (1994). إثبات الملكية في الوثائق العربية. ط1. القاهرة: الدار المصـــرية اللبنانية.

19- جمال الخولي. (2002). مداخلات في علم الدبلوماتيك العربي. ط2. الأسكندرية: دار الثقافة العلمية.

20- **حازم حسين.** (2010). الوثائق الدبلوماتيه الإلكترونيه : توثيقها وحجيتها . "أطروحة دكتوراه "، جامعة القاهره.

21- حسام الدين الأهواني. (1989). الحماية القانونية للحياة الخاصة في مواجهة الحاسب الإلكتروني. دراسه مقدمه إلى مؤتمر القانون والحاسب الآلي، الكويت.

22- حسناء على على عبد الغني . (2018). المعيار الدولي أيزو 17068 / 2012 موثوقية الطرف الثالث لتأمين الوثائق الرقمية : دراسة تحليلية وتطبيقية للمعيار في مصر . " أطروحة ماجستير"، جامعة الأزهر .

23- **حسناء على على عبد الغني** . (2022). علم الوثائق (الدبلوماتيك) وعلاقته بعلم الإثبات الجنائي الرقمي: دراسة نظرية وتطبيقية مقارنه. " أطروحة دكتوراه"، جامعة الأزهر .

24- حسن الحلوة. (1969). الدبلوماتيقا. مجلة كلية الآداب (جامعة القاهرة)، 27.

25- حسن ربيع. (2001). الإجراءات الجنائية في التشريع المصري. القاهرة: دار النهضة العربية.

26- **حسن عبد الباسط جميعى .** (2000) . إثبات التصرفات القانونيه التى يتم إبرامها عن طريق الإنترنت . القاهره : دار النهضة العربية.

27- دينا محمود عبد اللطيف محمد. (2017**).** الإتجاهات الحديثة فى علم الوثائق (الدبلوماتيك) ومجالات دراسته : دراسة تطبيقية . القاهرة : دار الفكر العربي.

28- سامي حمدان الرواشده.(2017). الأدلة المتحصلة من مواقع التواصل الإجتماعي ودورها في الإثبات الجنائي: دراسة في القانونين الإنجليزي والأمريكي. المجلة الدولية للقانون، 14 (3). متاح على الرابط التالي: https://www.qscience.com/docserver/fulltext/irl/2017/3/irl.2017.14.pdf?

29- سلوى على ميلاد. (1985). الوثيقة القانونية: ماهيتها – أجزاؤها – أهميتها. القاهرة: جامعة القاهرة، كلية الآداب.

30- سلوى على ميلاد.(2007) . قاموس مصطلحات الوثائق والأرشيف والمعلومات: إنجليزى – فرنسى – عربى . ط2 . القاهره : الدار المصريه اللبنانيه.

31- **سـلوى علي ميلاد.** (2018) . علم الوثائق (الدبلوماتيك) الحديث: رؤية لقواعد النقد الدبلوماتي من مابيون إلى دورانتي . مجلة الروزنامة، 15.

32- **الصـديق محمد الأمين الضـرير**. (2003). بطاقات الائتمان. دراسـه مقدمه إلى مؤتمر الأعمال المصـرفية الإلكترونية بين الشـريعة والقانون, مجموعة أعمال المؤتمر, المجلد الخامس, الإمارات العربيه المتحدة.

33- **طالب محمد جواد.** (2012). الحاسـب الجنائي: حاجة مُلحة في برامج دراسـة القانون والحاسوب. مجلة كلية الرافدين الجامعة للعلوم، (30).

34- **طاهري عبد المطلب.**(2015). الإثبات الجنائي بالأدلة الرقمية. "أطروحة ماجسـتير"، جامعة المسيلة.

35- **عائشـة أحمد حلمي عبدالعزيز**. (2018). نظـم إدارة وأرشـفـة البريد الإلكتـروني في المؤسسات الخاصة: دراسة تطبيقية."أطروحة ماجستير"، جامعة الأزهر.

36- **عبد الجبار الحنيص**. (2008). الحماية الجزائية لبطاقات الائتمان الممغنطة من التزوير. مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، 24(2).

37- **عبد الرزاق السـنهوري**.(1968) . الوسـيط في شـرح القانون المدني. ج 2 . القاهرة : دار النهضة العربية.

38- **عبـد الفتـاح بيومي حجـازي** .(2002). الـدليـل الجنـائي والتزوير في جرائم الكمبيوتر والإنترنت: دراسـة متعمقة في جرائم الحاسـب الآلي والإنترنت . القاهرة : دار الكتب القانونية.

39- **عبد الفتاح بيومي حجازي** . (2003). الإثبات في جرائم الكمبيوتر والإنترنت. القاهرة: دار الكتب القانونية.

40- **عمر محمد يونس** . (2008). الدليل الرقمي. القاهرة: دار النهضة المصرية.

41- **علي محمود علي حمودة** .(2003). الأدلة المتحصـلة من الوسـائل الإلكترونية في إطار نظرية الإثبات الجنائي . دراسـة مقدمة إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية. مركز البحوث والدراسات : أكاديمية شرطة دبي.

42- **عمر عبد السلام حسين الجبوري**.(2017). جريمة التزوير الإلكتروني في التشريع الأردني: دراسة مقارنة. "أطروحة ماجستير"، جامعة الشرق الأوسط.

43- **عمر فلاح العطين**. (2018). دور المحاكم الاقتصـادية في فض المنازعات التجارية. مجلة علوم الشريعة والقانون، 45 (4).

44- **فارس خطابي**. (2020). تزوير التوقيع الإلكتروني في بطاقات الائتمان: دراسـة على ضـوء القـانون 15 – 4 المتعلق بـالتوقيع والتصـديق الإلكترونيين. المجلـة الجزائريـة للأمن الإنساني، 5 (2).

45- **فاطمة الزهري خبازي**. (2017). جرائم الدفع الإلكتروني وسـبل مكافحتها. بحث مقدم في أعمال الملتقى الوطني لآليات مكافحة الجرائم الإلكترونية في التشـريع الجزائري، الجزائر، جامعة الجيلالي بونعامة، خميس مليانة. متاح على الرابط التالي:
http://jilrc.com/wp-content/uploads/2017.pdf

46- **محمد الأمين البشـري** (2005). التحقيق في جرائم الحاسـب الآلي. بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، كلية الحقوق والشريعة، جامعة الإمارات.

47- **محمد الأمين البشري**.(2008). تأهيل المُحققين في جرائم الحاسب الآلي وشبكات الإنترنت. المجلة العربية للدراسـات الأمنية والتدريب. جامعة نايف العربية للعلوم الأمنية – الرياض.

48- **محمد حسـين منصـور** . (2006). الإثبات التقليدى والإلكترونى . الأسـكندرية: دار الفكر الجامعى.

49- **معوض عبد التواب**. (1988). الوسـيط في شـرح جرائم التزوير والتزييف وتقليد الأختام. الأسكندرية: منشأة المعارف.

50- **ممدوح بن رشـيد الرشـيد العنزي**. (2015). الحماية الجنائية لبطاقات الدفع الإلكتروني من التزوير. المجلة العربية للدراسات الأمنية والتدريب، 31 (62).

51- **ممدوح عبد الحميد عبد المطلب**.(2003). أنموذج مقترح لقواعد اعتماد الدليل الرقمي للإثبات في الجرائم عبر الكمبيوتر. دراسه مقدمه إلى مؤتمر الأعمال المصرفيه الإلكترونيه بين الشـريعه والقانون , مجموعة أعمال المؤتمر , المجلد الخامس , الإمارات العربية المتحدة .

52- **ممدوح عبد الحميد عبد المطلب** .(2003). إسـتخدام بروتوكول TCP/IP في بحث وتحقيق الجرائم على الكمبيوتر . دراسـة مقدمة إلى المؤتمر العلمي الأول حول الجوانب القانونية

والأمنية للعمليات الإلكترونية، العدد 4، مركز البحوث والدراسات، الإمارات العربية المتحدة. متاح على الرابط التالي: https://www.f-law.net/law/threads/11321-

53- **ممدوح عبد الحميد عبد المطلب**.(2006). البحث والتحقيق الجنائي في جرائم الكمبيوتر والإنترنت: الجرائم عبر الكمبيوتر، البحث الجنائي العام، البحث الجنائي الخاص، الدليل الرقمي، مسرح الجريمة الواقعي. المحلة الكبرى: دار الكتب القانونية.

54- **وزارة العدل.** (2009). دليل إجراءات التقاضي لدى المحاكم الإقتصادية. متاح على الرابط التالي: http://www.jp.gov.eg/ar/LS.pdf

ثانياً - المراجع الأجنبية:

1- **Agarwal, A., Gupta, M., Gupta, S., & Gupta, S. C**. (2011). Systematic digital forensic investigation model. *International Journal of Computer Science and Security (IJCSS)*, *5*(1), 118-131.

2- **Aziz, B., & Blackwell, C. (2013, July)**. Use of KAOS in operational digital forensic investigations. In *Cyberpatterns 2013*.

3- **Carrier, B. (2003)**. Defining digital forensic examination and analysis tools using abstraction layers. *International Journal of digital evidence*, *1*(4), 1-12

4- **Casey, E. (2011)**. *Digital evidence and computer crime: Forensic science, computers, and the internet*. Academic press.

5- **Chasse, KL. (2007).** Electronic records as documentary evidence. Canadian Journal of Law and Technology.

6 - **Church, K., & De Oliveira, R. (2013, August)**. What's up with WhatsApp? Comparing mobile instant messaging behaviors with traditional SMS. In *Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services* (pp. 352-361).

7- **Ciardhuáin, S. Ó. (2004).** An Extended Model of Cybercrime Investigations. International Journal of Digital Evidence, 3(1), 1–22.

8 - Coe, P. (2015). The social media paradox: an intersection with freedom of expression and the criminal law. *Information & Communications Technology Law*, *24*(1), 16-40.

9 - Cohen, F. (2008/2014), *Digital Forensic Evidence Examination*, ASP Press.

10 - Cohen, F. (2009a), "Analysis of redundant traces for consistency", *IEEE International Workshop on Computer Forensics in Software Engineering (CFSE 09), Seattle, Washington*, 20-24 July.

11 - Cohen, F. (2009b), "Issues and a case study in bulk email forensics", *Fifth Annual IFIP WG 11.9 International Conference on Digital Forensics*, Orlando, FL.

12 - Cohen, F. (2009, May). Two models of digital forensic examination. In *2009 Fourth International IEEE Workshop on Systematic Approaches to Digital Forensic Engineering* (pp. 42-53). IEEE.

13 - Cohen, F. B. (2015). Digital diplomatics and forensics: going forward on a global basis. *Records Management Journal*, *25*(1), 21-44.

14 - Cohen, F. (2015). A Tale Of Two Traces—Diplomatics And Forensics. In *IFIP International Conference on Digital Forensics* (pp. 3-27). Springer, Cham.

15 - Croft, C. (2007). A brief history of the Facebook. *Retrieved from*: http://www.meerutcollege.org/mcm_admin/upload/1587223450.pdf

16 - Diamond, E. (1994). The archivist as forensic scientist: Seeing ourselves in a different way. *Archivaria*, *38*.

17 - Duranti, L. (1993). Origin and Development of the Concept of Archival Description. Archivaria,35(Spring), 47—54.

18 - Duranti, L. (1995). Reliability and authenticity: the concepts and their implications. *Archivaria*, *39*.

19 - Duranti, L. & MacNeil, H. (1996). The protection of the integrity of electronic records: an overview of the UBC-MAS research project, Archivaria, 42.

20 - Duranti, L. (1998). *Diplomatics: New Uses for an Old Science*, Scarecrow Press, Lanham, MD.

21 - Duranti, L., & Blanchette, J. F. (2004, January). The authenticity of electronic records: the InterPARES approach. In *Archiving Conference* (Vol. 2004, No. 1, pp. 215-220). Society for Imaging Science and Technology.

22 - Duranti, L. (2005). *The Long-term Preservation of Authentic Electronic Records: Findings of the InterPARES Project*. Archilab, San Miniato.

23 - Duranti, L., & Thibodeau, K. (2006). The concept of record in interactive, experiential and dynamic environments: the view of InterPARES. *Archival Science*, *6*(1), 13-68.

24 - Duranti, L. (2007). The InterPARES 2 Project (2002-2007): An Overview. *Archivaria*, *64*, 113-121.

25 - Duranti, L., & Preston, R. (2008). Research on Permanent Authentic Records in Electronic Systems (InterPARES) 2: Experiential. Interactive and Dynamic Records. Padova: Associazione Nazionale Archivistica Italiana.

26 - Duranti, L. (2009). From digital diplomatics to digital records forensics. *Archivaria*, *68*, 39-66.

27 - Duranti, L., & Endicott-Popovsky, B. (2010). Digital Records Forensics: A New Science and Academic Program for Forensic Readiness. Journal of Digital Forensics, Security and Law,5(2), 45–62. Retrieved from: http://www.jdfsl.org/subscriptions/JDFSL-V5N2-Duranti.pdf

28 - Duranti, L., & Jansen, A. (2011, August). Authenticity of digital records: an archival diplomatics framework for digital forensics. In *Proceedings of the 5th*

European Conference on Information Management and Evaluation (ECIME), Como (pp. 134-139).

29 - Duranti, L., & Rogers, C.(2012). Trust in digital records : An increasingly cloudy legal area . Computer law & Security review 28 , pp. 522 – 531.

30 - Foscarini, F. (2012). Diplomatics and genre theory as complementary approaches. *Archival Science*, *12*(4), 389-409.

31 - Ganesh, V. (2015). Digital Forensics. *International Journal* of advanced research, *3*(11).

32 - Honigman, B. (2012). 100 fascinating social media statistics and figures from 2012. *The Huffington Post*.

33 - Irons, A. (2006). Computer forensics and records management – compatible disciplines. *Records Management Journal*, 16 (2).

34 - ISO/IEC 7812-1:2017 specifies a numbering system for the identification of the card issuers, the format of the issuer identification number (IIN) and the primary account number (PAN).

35 - Jansen, A. (2015). Object-oriented diplomatics: Using archival diplomatics in software application development to support authenticity of digital records. Records Management Journal, 25 (1), p 45-55 Retrieved from: http://dx.doi.org/10.1108/RMJ-04-2014-0022

36 - Kirschenbaum, M., Ovenden, R., Redwine, G., & Donahue, R. (2010). Digital forensics and born-digital content in cultural heritage collections.

37 - Larsson, A. O. (2018). The news user on social media: A comparative study of interacting with media organizations on Facebook and Instagram. *Journalism studies*, *19*(15), 2225-2242.

38 - MacNeil, H. (1995). Metadata Strategies and Archival Description: Comparing Apples to Oranges. Archivaria, 39(Spring), 22–31.

39 - Mocas, S. (2004). Building Theoretical Underpinnings for Digital Forensics Research. Digital Investigation, 1(1). Retrieved from: http://www.elsevier.com/locate/diin (last visited 25 /5/ 2019).

40 - Montoya-Mogollón, J. B., & Troitiño Rodriguez, S. M. (2018). The Diplomatic and Digital Forensic Science in Born-Digital Records: The Quest for Authenticity. *Journal of Integrated OMICS*, *8*(1), 74-76.

41 - O'Floinn, M., & Ormerod, D. (2011). Social networking sites, RIPA and criminal investigations. *Criminal Law Review*, *2011*(10), 766-789.

42 - Palmer, G. (2001). A Road Map for Digital Forensic Research (DFRWS Technical Report). Retrieved from: http://www.dfrws.org/2001/dfrws-rm-final.pdf

43 - Palmer, G. L. (2002). Forensic analysis in the digital world. *International Journal of Digital Evidence*, *1*(1), 1-6.

44 - Palmer, I. N. (2018). *Forensic analysis of computer evidence* (Doctoral dissertation, University of Illinois at Urbana-Champaign).

45 - Parascandola, R. NYPD Forms New Social Media Unit to Mine Facebook and Twitter for Mayhem. The New York Daily News, August 10, 2011.

46 - Reith, M., Carr, C., & Gunsch, G. (2002). An examination of digital forensic models. *International Journal of Digital Evidence*, *1*(3), 1-12.

47 - Rogers, C.(2013). Digital Records Forensics: Integrating Archival Science into a General Model of the Digital Forensics Process . Proceedings of the Second International Workshop on Cyberpatterns: Unifying Design Patterns With Security, Attack and Forensic Patterns.

48 - Rogers, C. (2015). Diplomatics of born digital documents—considering documentary form in a digital environment. *Records management journal*, *25*(1), 6-20.

49 - Saferstein, R. (1998). *Criminalistics*: An Introduction to Forensic Science, Upper Saddle River, NJ: Prentice Hall.

50 - Shahid, S., & Zubairi, N. A. (2016). Comparative Study: An analysis of WhatsApp application and SMS by students & Professionals of Karachi. *Journal of Mass Communication Department, Dept of Mass Communication, University of Karachi*, *14*.

51 - Steppe, R. (2014). The freedom of speech on social networking services-Do we need protection against our own expressions?. *Jura Falconis*, *2013*(3), 559-589.

52 - Taylor, C., Endicott-Popovsky, B., and Frincke, D. (2007). Specifying Digital Forensics: A Forensics Policy Approach. I*n Proceedings of the 7th Digital Forensic Research Workshop*, Pittsburgh, PA, pp.101-104.

53 - Venter, H. S., & Kigwana, I. (2018). A digital forensic readiness architecture for online examinations. *South African Computer Journal*, *30*(1), 1-39.

54 - Walden, I. (2013). Accessing data in the Cloud: The long arm of the Law Enforcement Agent. In *Privacy and Security for Cloud Computing* (pp. 45-71). Springer, London. Retrieved from: http://www.wikayanet.dz/images/Documentation/Livres/PrivacySecurityCC.pdf

55 - Waterloo, S. F., Baumgartner, S. E., Peter, J., & Valkenburg, P. M. (2018). Norms of online expressions of emotion: Comparing Facebook, Twitter, Instagram, and WhatsApp. *new media & society*, *20*(5), 1813-1831. Retrieved from: https://journals.sagepub.com/doi/pdf/10.1177/1461444817707349

56 - Xie, S. (2011). Building foundations for digital records forensics: A comparative study of the concept of reproduction in digital records management and digital forensics. *The American Archivist*, *74*(2), 576-599.

57 - **Xie, S. L. (2013)**. Preserving digital records: InterPARES findings and developments. In *Financial Analysis and Risk Management* (pp. 187-206). Springer, Berlin, Heidelberg.

58 - **Zatyko, K .(2007).** Commentary: Defining Digital Forensics. Forensic Magazine (Feb/March), pp. 1–5.

The Approach and rules of digital diplomatics in the process of criminal proof of digital forensic records (Evidence): an applied study of information crimes

Dr. Hasnaa Ali Ali Abdeghany

Abstract

This study aimed to emphasize the role of Diplomatics in the process of digital forensic evidence, and the importance of the role of digital diplomatic criticism and its application to digital documents with the aim of emphasizing the validity of the procedures for obtaining digital documents (evidence), and how to reach the authenticity, validity, and integrity of documents and their non-disruption, or modification, alteration, or distortion, and the validity of its attribution to the offender in such a way that the judge relies on it in forming his belief and building his judgment. The study dealt with the application of the curriculum and rules of digital diplomatic criticism on models of digital documents (evidence) for information crimes in Egypt and the study of the research project for the criminal proof of digital documents (DRF).

The study concluded that, the congruences between the digital diplomacy approach and the digital forensic science approach are represented in evaluating the authenticity and defining the context, source, relationships, and meaning of digital documents (evidence). It also concluded the need to develop curricula and concepts that will allow specialists in documents, archives, information, law, and digital forensic sciences to identify documents in various digital environments.

Keywords: Digital Diplomatics; Digital Record; Information Crime; Digital Forensics