المركز الديمقراطي العربي
برلين - المانيا

الإكتشاف الإلكتروني & حجية الأدلة الرقمية في الإثبات

بين تحديات القبول وأمن المعلومات

اعداد:

د.أمل فوزى أحمد عوض

2022

المركز الديمقراطي العربي
برلين - المانيا

الإكتشاف الإلكتروني & حجية الأدلة الرقمية في الإثبات
بين تحديات القبول وأمن المعلومات

Democratic Arabic Center
Berlin - Germany

Electronic Discovery & Digital Evidence Authority
In proof between
The challenges of acceptance and information security

VR . 3383 – 6614 B

DEMOCRATIC ARABIC CENTER
Germany: Berlin 10315 Gensinger- Str: 112
http://democraticac.de
TEL: 0049-CODE
030-89005468/030-898999419/030-57348845
MOBILTELEFON: 0049174274278717

الـنـــــــــاشـــــــر:

المركز الديمقراطي العربي

للدراسات الاستراتيجية والسياسية والاقتصادية

ألمانيا / برلين

Democratic Arab Center

For Strategic, Political & Economic Studies

Berlin / Germany

لا يسمح بإعادة إصدار هذا الكتاب أو أي جزء منه أو تخزينه
في نطاق استعادة المعلومات أو نقله بأي شكل من الأشكال ،دون إذن مسبق خطي من الناشر.
جميع حقوق الطبع محفوظة

All rights reserved

No part of this book may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, without the prior written permission of the publisher.

المركز الديمقراطي العربي

للدراسات الاستراتيجية والسياسية والاقتصادية ألمانيا/برلين

Tel: 0049-code Germany

030-54884375

030-91499898

030-86450098

البريد الإلكتروني

book@democraticac.de

المركز الديمقراطي العربي
للدراسات الاستراتيجية، الاقتصادية والسياسية
Democratic Arabic Center
for Strategic, Political & Economic Studies

الكتاب : الإكتشاف الإلكترونى & حجية الأدلة الرقمية فى الإثبات بين تحديات القبول وأمن المعلومات

تأليف : د .أمل فوزى أحمد عوض

رئيس المركز الديمقراطي العربي: أ. عمار شرعان

مدير النشر: د. أحمد بوهكو

رقم تسجيل الكتاب: VR . 3383 – 6614. B

الطبعة الأولى

أذار / مارس 2022 م

الآراء الواردة أدناه تعبّر عن رأي الكاتب ولا تعكس بالضرورة وجهة نظر المركز الديمقراطي العربي

الإكتشاف الإلكترونى & حجية الأدلة الرقمية

فى الإثبات

بين تحديات القبول وأمن المعلومات

اعداد/

د.أمل فوزى أحمد عوض

دكتوراه فى القانون / كلية الحقوق / جامعة عين شمس
رئيس وحدة تكنولوجيا المعلومات - كلية التربية الفنية - جامعة حلوان

2022

الملخص:

تلعب البيانات دورًا مركزيًا لتطوير خوارزميات الذكاء الاصطناعي للاستخدام الفعلي فى مجال القانون وخاصة بالاكتشاف الإلكترونى للوصول الاسرع للبيانات القانونية والذى يحقق بالتبعية وصولا اسرع للعدالة، ولكن تطوير واستخدام خوارزميات الذكاء الاصطناعي مقيد بنقص البيانات التي يسهل الوصول إليها. فالمؤسسات والادارات والهيات القانونية غنية بالوثائق وفقيرة للبيانات " كالآراء القضائية إما لأنها غير متوفرة أو متنوعة في الشكل بحيث يصعب استخدامها بفعالية. بالإضافة إلى ذلك، يمكن أن تؤدي مجموعات البيانات ذات الجودة الرديئة أو المعيبة إلى قيام أنظمة الذكاء الاصطناعي بإخراج نتائج غير عادلة، وقد تؤدي تقنيات جمع البيانات، و إعدادها ، وتحليلها إلى تحيزات إحصائية في مجموعة البيانات . كما ان الإشكالية فيما يتعلق بالإثبات التي تثيرها الإستعانة بالوسائط الرقمية بالتقاضي هي إنه في الوضع العادي عندما يوجد ملف ورقي وآخر رقمي، فيمكن الوقوف علي صحة الأخير بمقارنته بالأول، أما في فرض البيئة الرقمية والدليل الرقمي كيف يمكن التحقق من سلامة بيانات مستند معين ؟ , وكيف يمكن التعويل علي الدليل الرقمي في الإجراءات عموما خاصة ان التبديل أو التعديل في الملفات الرقمية لا يترك أي أثر عليه ؟ وهل وجهة النظر القائلة بأن أي عيوب تتبدي بالنظام الرقمى لا يمكن ان تتساوي بحال من الأحوال مع الوضع قبل الإستعانة بتكنولوجيا المعلومات في القضاء علي صواب ؟ وكيف يمكن إنتقاء ايجابيات الدليل الرقمي والتعويل عليها ؟ وإتقاء سلبيات الدليل الرقمي ومعالجتها ؟ ، فـقد يتم التلاعب بمجموعات البيانات أو إتلافها عمدًا للحصول على تحليلات غير عادلة فـبالإضافة إلى مشكلات جودة البيانات ومعالجتها، تنشأ أيضًا مخاوف كبيرة بشأن خصوصية البيانات والأمن السيبراني مع استخدام كميات هائلة من البيانات بواسطة أنظمة الذكاء الاصطناعي. وجميع ما سبق يشكل تحديات غاية في الصعوبة أمام مستقبل الاكتشاف الإلكترونى والدليل الرقمى ... ترى كيف يتم التغلب عليها؟ وبأي الوسائل قانونية؟ أم تقنية ؟

الكلمات المفتاحية:

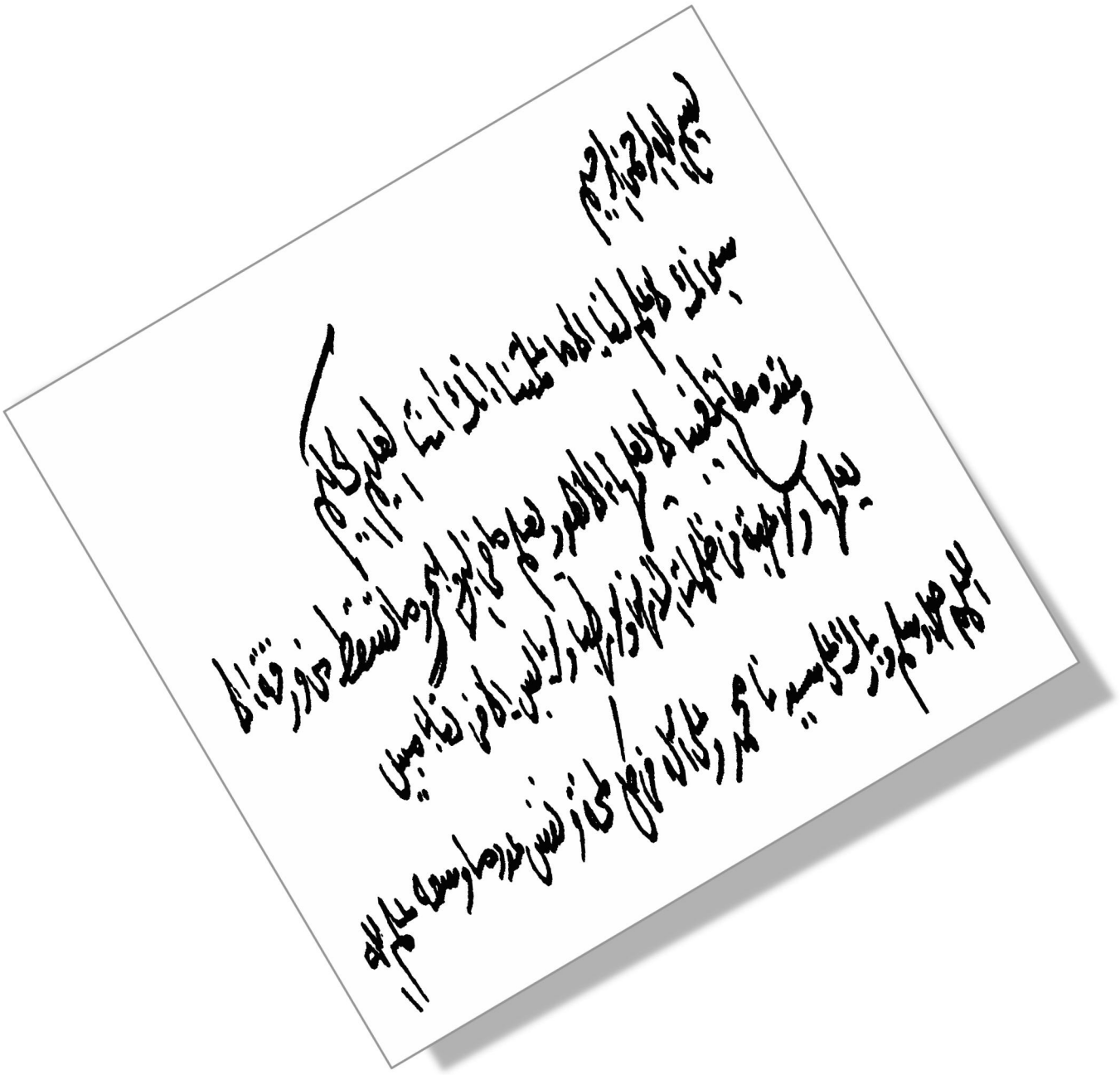
الاكتشاف الإلكترونى– الذكاء الاصطناعي– الدليل الرقمي – الطب الشرعى الرقمى – البيانات – معايير القبول – أمن المعلومات .

Summary:

Data play a central role in the development of artificial intelligence algorithms for actual use in the field of law, in particular in the electronic discovery of faster access to legal data, which, by extension, will achieve faster access to justice, but the development and use of artificial intelligence algorithms is constrained by a lack of easily accessible data. Institutions, departments and legal institutions are rich in documentation and poor data, "such as judicial opinions, either because they are not available or diverse in form and are difficult to use effectively. In addition, poor or flawed quality data sets can lead to unfair results from artificial intelligence systems and data collection, preparation and analysis techniques may lead to statistical biases in the data set. The problem with proof raised by the use of digital media in litigation is that, in the normal situation where a paper file and a digital file exist, the validity of the latter can be seen by comparing it to the former, but in the imposition of the digital environment and the digital directory, how can the integrity of the data of a particular document be verified? How can digital evidence be relied upon in procedures in general, especially since switching or modifying digital files leaves no impact on it? Is the view that any defects in the digital system cannot in any way be equated with the situation before the use of information technology to eliminate the right thing? How can the positives of the digital guide be selected and relied upon? To prevent and address the negatives of the Digital Guide? In addition to data quality and processing problems, there are also major concerns about data privacy and cybersecurity, with massive amounts of data being used by artificial intelligence systems. And all of the above poses very difficult challenges to the future of electronic discovery and digital evidence... You see how it's overcome? And by what legal means? Or tech?

Keywords:

Electronic Discovery, Artificial Intelligence, Digital Directory, Digital Forensic Medicine, Data, Acceptance Standards and Information Security.



إهـــــــــــــــداء

إذا جاء فضل الله وأنعامه تترا

فيكون الحمد والشكر يسعى

وأهدي الجهد والإجهاد صبرا

لأبي ثم امي عرفانًا وليس ردًا

وقبلهم الرسول حبيبنا وفخرا

به التمام والسند فضلًا وكرمًا

شكـــــــــر

الشكر موصولا لكل من علمني حرفا ما دمت حيا.....

مقدمة

بعد ما يقرب من 20 عامًا من الابتكار المستمر الذي يركز بشكل أساسي على الاكتشاف الإلكترونى ، يبدو أن التكنولوجيا القانونية تدخل مرحلة جديدة في حين أن المهنة القانونية ككل لا تزال متشككة إلى حد ما في التكنولوجيا وحذره من التغيير – خاصة عند مقارنتها بالصناعات الأخرى – في حين يقبل معظم المحامين الآن فرضية أن الأتمتة ضرورية لإدارة مكاتب المحاماة والإدارات القانونية بشكل أكثر كفاءة في ديناميكية بيئة أعمال شديدة التنافسية تعتمد على البيانات بشكل متزايد.[1]

وهو ما يترتب عليه ان يتغير فهمنا لما يجعل الأتمتة ضرورية ومهمة ، وحيث أن الاستثمارات في التكنولوجيا يمكن أن تكون فخًا ، مع وجود تكاليف باهظة للوصول السريع للبيانات ، في ظل التطور المستمر في تكنولوجيا المعلومات وتحديث البيانات.

تتعرض مكاتب المحاماة وعملائها من الشركات لضغوط هائلة لتقديم قيمة أكبر في مقابل أقل ولأن تكون أكثر عرضة للمساءلة أمام أصحاب المصلحة ، و يتم الشعور بهذا الضغط أيضًا بشكل حاد في قطاع التكنولوجيا القانونية ، حيث ستحتاج الشركات التي تبحث عن طريق إلى النجاح المستدام إلى تكييف نماذج أعمالها مع التطور المستمر في تكنولوجيا المعلومات وأمن البيانات. هذا ويترتب على استخدام تطبيقات تكنولوجيا المعلومات والتحول الرقمي في مجال القانون أن لدينا الكثير من الأدوات الرقمية لابد من الوقوف عليها والمعرفة بها ، فنحن كثيرًا ما ننقل البيانات من أداة إلى أخرى ، ونقوم باستمرار بتسجيل الدخول والخروج من تطبيقات متعددة ، وهذا يعني أيضًا أن البيانات الحساسة أكثر عرضة للضياع والتلف والاختراق

مشكلة البحث:

حيث تلعب البيانات دورًا مركزيًا لتطوير خوارزميات الذكاء الاصطناعي للاستخدام الفعلي فى مجال القانون وخاصة بالاكتشاف الإلكترونى للوصول الاسرع للبيانات القانونية والذى

---

[1] راجع فى ذلك :

https://www.lawtechnologytoday.org/2019/07/client-driven-innovation-the-future-of-legal-technology/

يحقق بالتبعية وصولا اسرع للعدالة، ولكن تطوير واستخدام خوارزميات الذكاء الاصطناعي مقيد بنقص البيانات التي يسهل الوصول إليها. فالمؤسسات والادارات والهيات القانونية غنية بالوثائق وفقيرة للبيانات " كالآراء القضائية إما لأنها غير متوفرة أو متنوعة في الشكل بحيث يصعب استخدامها بفعالية. بالإضافة إلى ذلك، يمكن أن تؤدي مجموعات البيانات ذات الجودة الرديئة أو المعيبة إلى قيام أنظمة الذكاء الاصطناعي بإخراج نتائج غير عادلة، وقد تؤدي تقنيات جمع البيانات، و إعدادها ، وتحليلها إلى تحيزات إحصائية في مجموعة البيانات . كما ان الإشكالية فيما يتعلق بالإثبات التي تثيرها الإستعانة بالوسائط الرقمية بالتقاضي هي إنه في الوضع العادي عندما يوجد ملف ورقي وآخر رقمي، فيمكن الوقوف علي صحة الأخير بمقارنته بالأول، أما في فرض البيئة الرقمية والدليل الرقمي كيف يمكن التحقق من سلامة بيانات مستند معين ؟ , وكيف يمكن التعويل علي الدليل الرقمي في الإجراءات عموما خاصة ان التبديل أو التعديل في الملفات الرقمية لا يترك أي أثر عليه ؟ وهل وجهة النظر القائلة بأن أي عيوب تتبدي بالنظام الرقمى لا يمكن ان تتساوي بحال من الأحوال مع الوضع قبل الإستعانة بتكنولوجيا المعلومات في القضاء علي صواب ؟ وكيف يمكن إنتقاء ايجابيات الدليل الرقمي والتعويل عليها ؟ وإتقاء سلبيات الدليل الرقمي ومعالجتها ؟ ، فـقد يتم التلاعب بمجموعات البيانات أو إتلافها عمدًا للحصول على تحليلات غير عادلة فـبالإضافة إلى مشكلات جودة البيانات ومعالجتها، تنشأ أيضًا مخاوف كبيرة بشأن خصوصية البيانات والأمن السيبراني مع استخدام كميات هائلة من البيانات بواسطة أنظمة الذكاء الاصطناعي. وجميع ما سبق يشكل تحديات غاية في الصعوبة أمام مستقبل الاكتشاف الإلكترونى والدليل الرقمى ... ترى كيف يتم التغلب عليها؟ وبأي الوسائل قانونية؟ أم تقنية ؟

أن أول ما يُطرح في موضوع الإثبات هو توفر السند الخطي, سواء كُتب بخط اليد أو بالآلة الكاتبة, وما يحتويه من البيانات, وتوقيع أطرافه, وتعدد النسخ في العقود المتبأدلة ، والشكل الذي قد يفرضه القانون في حالات معينة.

هذا بالاضافة إلي معضلة تحديد القانون الواجب التطبيق علي العقود الرقمية الدولية وقوتها الثبوتية ، وإشكالية إستعماله ، وإثباته، وطريقة تقديمه للمحكمة الناظرة في النزاع المتعلق به. وكذلك اشكالية تحديد مفهوم أصل السند الرقمي وصورته؛ إذ أن النسخة هي تكرار الأصل في كل جزئياته, لذلك تعتبر النسخة أصلاً جديداً من دون تمييز بينهما.

لكن التساؤل الأساسي1 في هذا الصدد والذي يستتبع تبني الإستعانة بالوسائل الرقمية في التقاضي هو:

- **كيف يمكن ان يضمن إستخدام الوسائل الحديثة السرية والرسمية في ذات الوقت للملفات التي يتم تبادلها رقميا سواء بين المحكمة والخصوم أو الخصوم بعضهم البعض؟**
- **هل هذه الآليات- أي الوسائل الرقمية- علي درجة من الكفاءة بحيث يمكن الإعتماد عليها في ضمان سلامة البيانات وأمن المعلومات المتداولة رقميا؟[2]**
- **كيف يمكن التحكم في الصعوبات المرتبطة بإستخدام التكنولوجيا دون الإخلال بالتنظيم القضائي والضمانات الأساسية لحسن سير العدالة؟[3]**

ذلك ان الإشكالية 4 فيما يتعلق بالإثبات التي تثيرها الإستعانة بالوسائل الرقمية5 في التقاضي هي إنه في الوضع العادي عندما يوجد ملف ورقي وآخر رقمي، فيمكن الوقوف علي صحة الأخير بمقارنته بالأول، أما في فرض البيئة الرقمية والدليل الرقمي كيف يمكن التحقق من سلامة بيانات مستند معين (ويمكن التعويل عليه في الإجراءات عموما خاصة ان التبديل أو

---

[1] راجع فى ذلك : د/فاطمةعادل سعيد "التقاضي عبر وسائل التكنولوجيا والاتصال الحديث " , بحث مقدم الى مؤتمرالقانون واللتكنولوجيا – كلية الحقوق – جامعةعين شمس , فى الفترة من 8 الى 10 ديسمبر 2017.

[2] يقصد بمصطلح **سلامة البيانات:** "التحقق من ان البيانات التى تضمنتها الوثيقة لم يحدث بها أى تعديل أو حذف سواء لأسباب طبيعية أو عمدية." راجع د.محمد محمد سادات ،. حجية التوقيع الرقمى فى الاثبات ، رسالة دكتوراه ، ج. المنصورة ، ٢٠١٠ ، ص ١٩٥

3راجع فى ذلك : أسامة المناعسة وآخرون ؛ د. هلالي عبداللاه أحمد ، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي . دراسة مقارنة ، الطبعة الأولى ، دار النهضة العربية . القاهرة ، 1997 ، وقد آثرنا الاشارة دون الافاضة لعدم اتساع المجال لذلك.

[4] Helmut Rü mann, Electronic Documents. Security and Authenticity, Electronic Technology and Civil Procedure- New Paths to Justice from Around the World, Springer, 2012, p.235.

[5] راجع فى ذلك كلا من :

-Walker, Janet, and Garry D. Watson. "New Trends in Procedural Law: New Technologies and the Civil, Litigation Process." Hastings International and Comparative Law Review 31.1 (2008), http://www.delmarlearning.com/companions/content/1401824293/guides/CH6.

التعديل في الملفات الرقمية لا يترك أي أثر عليه و العكس1) من هذا النقد يري البعض ان أي عيوب تتبدي في النظام الرقمي لا يمكن ان تتساوي بحال من الأحوال مع الوضع قبل الإستعانة بتكنواوجيا المعلومات في القضاء .

إن الذي يضفي الرسمية علي الأوراق / المستندات في النظام الورقي هو التوقيع، وهو نفس الآلية التي سوف يعتمدها المشرع لإضفاء الرسمية علي المحررات الرقمية.

أهداف البحث:

1. الوقوف علي ماهية إدارة المعلومات الذكية لإدارة الخصومة القضائية رقميًا " من خلال عملية الاكتشاف الإلكترونى ،E – discovery والذي يتم تعريفه على أنه عملية الاكتشاف في التقاضي المدني الذي يتم تنفيذه بتنسيقات رقمية ،[2] وهي تشمل ما يشار إليه غالبًا بالمعلومات المخزنة رقميًا أو ESI .
2. الوقوف على أهم مصطلحات الإثبات الرقمى : كالدليل الرقمى , التوقيع الرقمى ، المحررات الرقمية
3. التعرض بالضروة لبعض الجوانب الفنية بالقدر اللازم كأليات التوثيق، التشفير.
4. الوقوف على أهم إشكاليات قبول الأدلة بالإثبات الرقمى.

منهج البحث:

سوف نستخدم في هذه الورقة البحثية المنهج التحليلي والتأصيلي لعرض مسائله وطرح المعالجات والحلول الملائمة.

خطة البحث:

سوف نطرح معالجات للتساؤلات السابق ذكرها على مستوى عدد من المباحث على النحو التالى :

---

[1]Jay Thornton, (Cost, Accuracy, and subjective fairness in legal information technology: a response to technological due process critics), New York university law review, December 2016, Vol.91, p.

[2]راجع فى ذلك:

"The transformation of civil justice to digital advantages between difficulties and challenges " , BISKRA UNIVERSITY – FACULTY OF LAW AND POLITICAL SCIENCES Laboratory impact of jurisprudence on the dynamics of legislation, Jurisprudence Journal .– Vol 12 – (Special Issue) – September 2020

المبحث الأول: الاكتشاف الإلكترونى

المطلب الأول: ماهية الاكتشاف الإلكترونى و الإدارة الذكية للمعلومات

المطلب الثانى: متطلبات الاكتشاف الإلكترونى

المطلب الثالث: تحديات الاكتشاف الإلكترونى

المطلب الرابع: التخطيط الناجح الاكتشاف الإلكترونى

المطلب الخامس: الذكاء الاصطناعي والاكتشاف الإلكترونى

المبحث الثانى : الأدلة الرقمية

المطلب الأول : ماهية الأدلة الرقمية

المطلب الثاني : متطلبات الإثبات بالأدلة الرقمية

المطلب الثالث : أنواع الأدلة الرقمية

المطلب الرابع : تحديات قبول الأدلة الرقمية

المطلب الخامس: موقف النظم القضائية المقارنة

المبحث الأول

الاكتشاف الإلكترونى[1]

وللوقوف على ماهية الاكتشاف الإلكترونى ومعرفة ما اذا كان مزايا ام تحديات سوف نعرض إدارة المعلومات الذكية والاكتشاف الإلكترونى ،ثم نعرض للتخطيط الناجح الاكتشاف الإلكترونى ،كما سنعرض لمتطلبات الاكتشاف الإلكترونى ،والذكاء الاصطناعي والاكتشاف الإلكترونى ، وتحديات الاكتشاف الإلكترونى وذلك على النحو التالى:

المطلب الأول: ماهية الاكتشاف الإلكترونى و الإدارة الذكية للمعلومات

المطلب الثانى: متطلبات الاكتشاف الإلكترونى

المطلب الثالث: تحديات الاكتشاف الإلكترونى

المطلب الرابع: التخطيط الناجح الاكتشاف الإلكترونى

المطلب الخامس: الذكاء الاصطناعي والاكتشاف الإلكترونى

[1] راجع فى ذلك : د/أمل فوزى أحمد ،بحث بعنوان "الإكتشاف الإلكترونى ، والوصول الأسرع للعدالة مزايا أم تحديات؟" ، المؤتمر الدولى الأول ، تحت عنوان " التحولات الرقمية : التأثيرات والتحديات " ، كلية العلوم القانونية ،والاقتصادية ، والاجتماعية ، بتطوان ، جامعة عبد المالك السعدى ، المغرب ، يومى 9و10 يونيو 2021.

المطلب الأول

ماهية الاكتشاف الإلكترونى E – DISCOVERY و الإدارة الذكية للمعلومات

اولا :ما هو الاكتشاف الإلكترونى E – discovery؟[1]

الاكتشاف هو المصطلح المستخدم للمرحلة الأولية من التقاضي حيث يتعين على الأطراف في النزاع تقديم المعلومات والسجلات الأخرى ذات الصلة ، إلى جانب جميع الأدلة الأخرى المتعلقة بالقضية .المفتاح لمعالجة E – discovery هو أن تكون استباقيًا في إدارة المعلومات والسجلات مع التحكم في معالجة طلبات E – discovery المحتملة. فالمقصود من تبادل الأدلة والمستندات هو[2] تسليم صورة من المذكرة بالمناولة للخصم أو وكيله مع توقيع المستلم علي الأصل قبل تقديمها للمحكمة ، في حين أن الأصل أن يتم إيداع المذكرة في مكتب إدارة الدعوي بالمحكمة المختصة (سواء أكانت محكمة أول درجة أو محكمة ثاني درجة) ويتم إبلاغ الخصم بذلك الإيداع ويتم اطلاعه عليها في ملف القضية بمكتب إدارة الدعوي ، كما يترتب علي إيداع مذكرة الدفاع اعتبار المدعي عليه حاضراً حكماً ولو تخلف عن الحضور . وتري الباحثة إنه يجب تعديل نصوص القانون بما يسمح للخصوم بالتقديم والتبادل والاطلاع علي هذه المستندات رقميا[3]. وهو ما يعرف الآن بالإكتشاف الإلكترونى ،[4]والذي يعد من تطبيقات

---

[1] راجع في ذلك كلا من:

- https://en.wikipedia.org/wiki/Electronic_discovery
- https://www.exterro.com/basics-of-e-discovery
- https://www.logikcull.com/what-is-ediscovery-software
- https://www.exterro.com/basics-of-e-discovery/e-discovery-process
- https://www.logikcull.com/guide/introduction-to-ediscovery-basics
- https://www.aiim.org/what-is-ediscovery
- https://cdslegal.com/knowledge/the-basics-what-is-e-discovery/
- https://bok.ahima.org/doc?oid=107115#.YDekLujXLx4

[2] راجع في ذلك : د/ سيد احمد محمود ،"نحو رقمية القضاء المدني الاماراتي" ،ص327.

[3] راجع في ذلك :

- كيفية إرسال مستندات المحكمة المدنية:
- https://docplayer.net/13527036-File-how-to-transmit-civil-court-documents-by-fax-for-filing-in-court-registries-in-b-c-transmitting-by-fax-court-services-court-services-branch.html (تاريخ آخر دخول علي الموقع 2020/9/22

التقاضي الرقمي، ويتم تعريف الإكتشاف الإلكترونى علي أنه العملية القانونية السابقة الأطراف علي المعلومات المخزنة رقميًا ومراجعتها، وهو إجراء مطبق بالنظم القضائية المقارنة حيث عملت القواعد الفيدرالية للإجراءات المدنية لعام 2006 (FRCP) علي وضع المعلومات المخزنة رقميًا (ESI) علي قدم المساواة مع المستندات الورقية في نظر المحكمة[1].

يمكن استخدام 2ESI أي نوع من بيانات أو الأجهزة ESI بما في ذلك علي سبيل المثال لا الحصر ، النصوص ،والصور ،والصوت ،وقواعد البيانات ،وجداول البيانات ،والأنظمة القديمة ،والشريط، والهواتف الذكية، والأجهزة اللوحية، والرسائل الفورية ،والبريد الرقمي، وملفات التقويم ،ومواقع الويب[3].

– دليل مستخدم نظام ملفات الحالة الرقمية :

– https://docplayer.net/9703973-Electronic-case-files-system-user-s-manual.html(تاريخ آخر دخول علي الموقع 2020/9/22)

– معالجة النماذج الرقمية :

– https://docplayer.net/14451754-Electronic-forms-processing-eforms.html2020/9/22 تاريخ آخر دخول علي الموقع)

[4] راجع في ذلك :

Mikl s Kengyel; Zolt n Nemess nyi; International: Electronic technology and civil procedure : new paths to justice from around the world,p285.

http://www.worldcat.org/title/electronic-technology-and-civil-procedure-new-paths-to-justice-from-around-the-world/oclc/773670695

[1] راجع في ذلك :

– Legal Technology Vision Towards the digital transformation of the legal sector , Legal Technology Cluster Committee , Singapore Academy of Law , p33

– https://bok.ahima.org/doc?oid=107115#.YDekLujXLx4 تاريخ آخر دخول علي الموقع 21/2/2021

[2] راجع في ذلك :

— Ediscovery And Digital Forensics , Solving Legal And Regulatory Issues , P1-6 , Cyber@Bsigroup.Com , Bsigroup.Com

[3] راجع في ذلك :

فالإكتشاف الإلكترونى ISE (électronica Discovery)[1] يشبه إلي حد كبير E-filing ، هو موجة الحاضر والمستقبل، وتحدي للواقع أيضاً[2] .

ثانيا : التكوين الحقيقي لحركة إدارة المعلومات والبيانات[3]

دون علم الكثيرين ، فإن الأصل الحقيقي لحركة إدارة المعلومات والبيانات اليوم يكمن في دعوى التمييز بين الجنسين العادية التي رفعتها متداولة الأوراق المالية لورا زوبولاك في المنطقة الجنوبية من نيويورك .(SDNY) عندما رفعت متداولة الأوراق المالية ، لورا زوبولاكي دعوى قضائية ضد صاحب عملها ، يو بي إس واربورغ ، في عام 2002 ، لم يكن من المحتمل أن يفهم يومًا ما أنها ستعرف بأنها رائدة في حركة إدارة المعلومات والبيانات اليوم – أو أن قضيتها ستؤثر وتغير الطريقة إلى الأبد يدير المستشار القانوني والمنظمات التي يمثلونها معلوماتهم

— ADAM I. COHEN, DAVID J. LENDER, ELECTRONIC, DISCOVERY, PRACTICE, GUIDELINES, p2-37

[1] راجع في ذلك :

— AHIMA. "E- Discovery Litigation and Regulatory Investigation Response Planning: Crucial Components of Your Organization's Information and Data Governance Processes." Journal of AHIMA 84, no.11 (November–December 2013): expanded web version , p 1-91 .

[2] راجع في ذلك :

— e-Discovery: What Litigation Lawyers Need to Know , Risk Management Practice Guide of Lawyers Mutual, LAWYERS MUTUAL LIABILITY INSURANCE COMPANY OF NORTH CAROLINA , p 2-17, www.lawyersmutualnc.com

[3]راجع فى ذلك :

— https://www.google.com/search?sxsrf=ALeKk03chjd_CNkdk1Fnsot6owkUFOs-4Q:1622449002937&q=Digital+Evidence+and+Computer+Crime:+Forensic+Science,+Computers+and+the+Internet&stick=

وبياناتهم – أو قد تكون العواقب المترتبة على المعالجة غير الصحيحة للمعلومات المخزنة رقميًا من قبل المستشار القانوني أو الادارة التي يمثلونها في سياق التقاضي وخيمة.

حتى يومنا هذا ، بالنسبة إلى قرارات Zubulake ،[1]تعد قرارات من أهم قرارات القانون (إن لم تكن الأكثر أهمية) بشأن إدارة المعلومات والبيانات في عصرنا، و أربعة من خمسة من هذه القرارات أثرت على تعديلات FRCP لعام 2006 ، وكذلك العديد من تعديلات 2013 المقترحة على FRCP لإدارة الاكتشاف الإلكترونى بنجاح.

عملية E – discovery القانونية – تعمل E – discovery من وقت رفع الدعوى حتى وقت تقديم الدليل الرقمي في المحكمة كما يلي:[2]

1. يتم تحديد البيانات على أنها ذات صلة من قبل المحامين ويتم وضعها قيد الحجز القانوني.
2. يقوم المحامون من كلا الجانبين بتحديد نطاق الاكتشاف ، وتحديد ESI ذي الصلة ، وتقديم طلبات E – discovery .
3. يمكن التفاوض مع المستشار القانوني لتحديد ما يتم البحث عنه وللتأكد من تحديد الأدلة المطلوبة واستبعاد عدم وجود أدلة ، وبالتالي تقليل الجهد الإجمالي المطلوب للبحث والمراجعة وتقديمه.

---

[1]راجع في ذلك:

- https://nydailyrecord.com/2013/07/22/an-interview-with-laura-zubulake/,
- https://www.relativity.com/blog/the-end-of-an-e-discovery-era-judge-scheindlins-law-from-zubulake-to-today/,
- https://en.wikipedia.org/wiki/Zubulake_v._UBS_Warburg,
- https://cloudnine.com/ediscoverydaily/case-law/ediscovery-history-a-look-back-at-zubulake/,
- https://www.larkinhoffman.com/files/OTHER/bjd_ppp_elecdis.pdf

[2]راجع في ذلك :التحول الرقمي: الآثار الرئيسية لخدمات وعروض تكنولوجيا شركة المحاماة

— https://www.lawtechnologytoday.org/2019/05/digital-transformation-key-implications-for-law-firm-technology-services-and-offerings

4. ثم يتم استخراج الأدلة وتحليلها باستخدام إجراءات الطب الشرعي الرقمية ، والتي عادة ما يتم تحويلها إلى صيغة PDF[1] أو TIFF[2] لاستخدامها في المحكمة.

مفتاح النجاح مع E – discovery هو أن يكون لديك سياسة تشدد على:

- التخلص من المعلومات التي ليس لها قيمة تجارية وفقًا للسياسة وفي سياق العمل العادي
- تخزين السجلات التي لها قيمة للمؤسسة وإدارتها بشكل صحيح ، تحت سيطرة الادارة.
- تنفيذ مخطط التصنيف الذي يوفر بنية إدارة المعلومات والسجلات لتحقيق الاتساق والتحكم .
- تدمير السجلات التي لم تعد هناك حاجة إليها بطريقة منهجية وموثقة وآمنه.

كما تُمكِّن تطبيقات E – discovery[3] المؤسسات من سحب المعلومات والسجلات من الأحجام الهائلة للمحتوى ، بما في ذلك رسائل البريد الرقمي .

ثالثا :ما هي إدارة المعلومات والبيانات؟

في مارس 2013 ، أنشأت جمعية إدارة المعلومات الصحية الأمريكية (AHIMA)[4] وقدمت تعريفاتها الخاصة للمعلومات الصحية وإدارة البيانات[5] ، والتي يعد الاكتشاف الإلكترونى والتخطيط للاستجابة للتقاضي من مكوناتها .

---

[1]صيغة الPDF هي صيغة رقمية للملفات صممتها أنظمة ال Adobe باستخدام بعض الأكواد الملحقة بخصائص اللغات. يأتي البرنامج الرسمي لمشاهدة الملفات بصيغة ال Adobe Reader. و عادة ما يكون ملف ال PDFدمجًا بين النصوص ذات الرسوميات التسامتية و الموجّهة و النصوص و النصوص المكتوبة بالجافا و عناصر أخرى.

[2]الTIFF : هي صيغة لتخزين الرسوميات النقطية. تُستخدّم للمسح الضوئي و في مجال نصوص ال OCR، لإرسالها بالفاكس وطباعتها كما أنه مدعوم من العديد من التطبيقات الرسومية. طوّرت الصيغة شركةAldus بالتعاون مع مايكروسوفت لاستخدامها مع الأكواد اللاحقة بالصيغة المستخدّمة لتخزين الصور بعمق رائع للون ،و التي تمتلك حقوق النشر الخاصة بها أنظمة أدوبي.

[3] https://www.getapp.com/legal-law-software/electronic-discovery/

[4] AHIMA. "E- Discovery Litigation and Regulatory Investigation Response Planning: Crucial Components of Your Organization's Information and Data Governance Processes." Journal of AHIMA 84, no.11 (November–December 2013): expanded web version.

[5] https://library.ahima.org/doc?oid=301489#.YL9d_PnXIak

رابعا : التحضير لعقد اجتماع ما قبل المحاكمة [1]

سيشرف قاض على التقاضي بشأن الاكتشاف الإلكترونى بين الأطراف .قبل المحاكمة[2] ، يجتمع المستشار القانوني للأطراف ويتشاور مع القاضي لمناقشة الأمور والاتفاق عليها فيما يتعلق باكتشاف[3] المعلومات الرقمية. يمكن إجراء جلسات اللقاءات والندوات في جلسة واحدة أو عدة جلسات ، و يعتمد العدد الفعلي للجلسات على العديد من العوامل التي تؤثر على القضية ، بما في ذلك حجم القضية ونطاقها وتعقيدها بالإضافة إلى معرفة وتعليم وخبرة القاضي ومعاونيه والمحامين المشاركين في التقاضي بالاكتشاف الإلكترونى ، ونظرًا للكميات الهائلة من المعلومات الرقمية الموجودة داخل أنظمة المعلومات اليوم ، يمكن أن يكون الاكتشاف الإلكترونى عملية معقدة وتستغرق وقتًا طويلاً ومكلفة .لذلك ، قبل عقد مؤتمر ، e-discovery and confer من المهم أن يكون المستشار القانوني على دراية بأنظمة المعلومات وسياسات إدارة[4] السجلات.

وفي عالم ESI اليوم ، فإن دور المسئول الرسمي عن حفظ البياتات ليس واضحًا و هو ما سيترتب عليه حدوث مشكلات تتعلق بالاحتفاظ بالمعلومات المخزنة رقميًا وحفظها وإنتاجها .لذلك ، يجب على الجهات الفاعلة إنشاء ومراقبة سياسات وإجراءات الحجز القانوني المكتوبة التي توضح كيفية حفظ السجلات والاحتفاظ بها في مواجهة التقاضي أو التحقيق ، وتقدم ESI أربعة مستويات أساسية لحماية البيانات على النحو التالى[5] :

---

[1] راجع فى ذلك : د.أمل فوزى أحمد:

- بحث بعنوان " آليات فعالة للتحول الآمن بالنظم القضائية الى الرقمية" ، المؤتمر العلمي الخامس (الافتراضي) ، كلية الحقوق جامعة السلطان قابوس ، " نظم التقاضي وتحديث قواعد الاثبات "تطوير نظم التقاضي وتحديث قواعد الإثبات" ، ٢٢ ديسمبر ٢٠٢٠.
- بحث بعنوان " المهارات الفنية والقانونية لإدارة الخصومة القضائية رقميا" ، المؤتمر العلمي الخامس (الافتراضي) ، كلية الحقوق جامعة السلطان قابوس ، " نظم التقاضي وتحديث قواعد الاثبات "تطوير نظم التقاضي وتحديث قواعد الإثبات" ، ٢٢ ديسمبر ٢٠٢٠.

[2] https://library.ahima.org/doc?oid=301993#.YL9d1_nXIak

[3] https://library.ahima.org/doc?oid=301981#.YL9d7_nXIak

[4] https://library.ahima.org/searchresults?fqa=CategoryIdsAllHierarchical|{5B64421A-6F43-4FC1-B278-9EA38EA92210}&s=3&v=1&num=10

[5] AHIMA. "E- Discovery Litigation and Regulatory Investigation Response Planning: Crucial Components of Your Organization's Information and Data Governance

مستويات الحماية:

تقدم المعلومات المخزنة رقميًا للمنظمات أربعة[1] مستويات من الحراسة على السجلات .تعتمد هذه على علاقة الشخص أو الكيان بنظام البيانات والقرب من القضية في التقاضي .كما هو الحال في السجلات الورقية التقليدية.

المستوى 1: الأمناء الأساسيون أو المباشرون :هؤلاء الأشخاص الذين يتعاملون مع البيانات بشكل مباشر أو لديهم مشاركة مباشرة أو على علم بأحداث القضية .

المستوى 2: مالكو البيانات أو المضيفون: قد يتم تعيين الأفراد المسؤولين عن الإشراف على مناطق عمليات الأعمال كمالكين للبيانات أو مضيفين لديهم معرفة بالإجراءات المستخدمة لإنشاء أنواع معينة من السجلات وإدارتها وحفظها .

المستوى 3: شركاء الأعمال والأطراف الثالثة: المتعاقدون وغيرهم ممن يؤدون مجموعة متنوعة من الوظائف المرتبطة بمعلومات الطرف ولكن ليسوا أطرافًا في التقاضي .تشمل الأمثلة مزودي خدمة الإنترنت وموفري خدمات التطبيقات مثل غرفة مقاصة المطالبات وموفري الخدمات الآخرين الذين يقدمون خدمات تتراوح من تخزين البيانات خارج الموقع إلى الاستعانة بمصادر خارجية كاملة لقسم تكنولوجيا المعلومات.

المستوى 4: السجل الرسمي وأمناء النظام[2]: يجب على كل منظمة تحديد الخطوط العريضة

Processes." Journal of AHIMA 84, no.11 (November–December 2013): expanded web version.

[1]راجع فى ذلك :

التقاضي الرقمي والتخطيط للاستجابة للتحقيق التنظيمي: المكونات الحاسمة لمعلومات مؤسستك وعمليات إدارة البيانات:

https://bok.ahima.org/doc?oid=107115#.YDekLujXLx4

[2]راجع فى ذلك :

خمس طرق لاستعادة التحكم في مستنداتك بعمليات الأعمال المكثفة

https://www.lawtechnologytoday.org/2020/02/5-ways-to-retake-control-of-your-document-intensive-business-processes

الأعمال الصغيرة: تدابير اختبار الأمن السيبراني

كجزء من التقاضي.

فقد يكون الموظفون داخل قسم تكنولوجيا المعلومات بمثابة الحارس الرسمي لنظام المعلومات،و تشمل الأمثلة على ذلك أجهزة الكمبيوتر والخوادم وأنظمة النسخ الاحتياطي والقديمة وأنظمة الاتصالات والصوت والوسائط القريبة ، و سيلعب موظفو تكنولوجيا المعلومات الذين يعملون بهذه الصفة دورًا أساسيًا في اكتشافESI .

يدير هؤلاء الموظفون البنية التحتية التقنية لأنظمة إدارة المعلومات على أساس يومي ،و يفهمون العلاقات العامة بين الملفات المختلفة ، وآليات التخزين لأنظمة إدارة المعلومات على المستوى التقني.

وحيث أصبح البريد الرقمي هو المعيار الفعلي للاتصالات عبر المؤسسات يجب على كل مؤسسة خاصة مؤسسات الرعاية الصحية أن تضع وتنفذ نوعًا من السياسة فيما يتعلق باستخدام نظام إدارة البريد الرقمي.

ففي الاختصاصات القضائية للقانون العام والقانون المدني[1] ، يستخدم الأطراف بشكل متزايد E discovery –لإجراء **مشاريع معقدة وكبيرة الحجم للكشف عن المستندات** ، ولا يمكن للأطراف القيام بذلك إلا بطريقة فعالة من حيث التكلفة وسليمة من الناحية الجنائية ، مع إدارة المخاطر القانونية بشكل مناسب.

https://www.lawtechnologytoday.org/2021/05/small-business-cyber-security-testing-measures

[1]راجع فى ذلك : د.أمل فوزى أحمد ، بحث بعنوان " تحديات العدالة الرقمية أمام المحاكم المدنية " منشور بمجلة الدراسات والبحوث القانونية عدد جوان 2020.

المطلب الثانى

متطلبات الاكتشاف الإلكترونى[1]

ما يتم تجاهله أحيانًا في صياغة طلبات الاكتشاف والتفاوض بشأنها هو *شكل* إنتاج المستندات، و يمكن أن يؤدي تحديد شكل الأدلة الرقمية بالاكتشاف إلى توفير قدر كبير من الوقت والمال في مرحلة مراجعة المستندات ويؤدي إلى إنتاج بيانات قيمة لن يتم إنتاجها على الإطلاق.

اولا : البيانات الوصفية

يجب أن تحتوي جميع عمليات إنتاج المستندات الرقمية ، واستخراج الأدلة الرقمية على بعض حقول البيانات الوصفية الأساسية ، بما في ذلك:

- اسم الملف
- تعديل التواريخ
- تاريخ إرسال البريد الرقمي
- مؤلف الرسالة
- التعديل الأخير من قبل المرسل
- المستلمون (بما في ذلك النسخ المخفية (نسخة مخفية الوجهة))
- مسار المصدر
- سطر الموضوع

الغرض من البيانات الوصفية هو الحفاظ على المعلومات حول المستندات التي قد تضيع إذا تم إعادة معالجتها.

لا توفر هذه المعلومات حقائق أساسية غير واضحة من المستند فحسب ، بل تساعد أيضًا في المراجعة الفعالة والدقيقة للوثائق ، ويعد تحليل البيانات الوصفية أحد الطرق الرئيسية التي يمكن

---

[1] راجع فى ذلك :

https://www.lawtechnologytoday.org/2017/08/e-discovery-request-youre-requesting/

لفريق مراجعة المستندات من خلالها التعرف بذكاء على المستندات ذات الاهمية دون الحاجة إلى الانخراط في مراجعة خطية يدوية.

ثانيا :تنسيق المستندTIFFs[1]

في حين أن تنسيق TIFF هو شكل مقبول من أشكال الإنتاج للعديد من المستندات ، يجب إنتاج أنواع معينة من الملفات بتنسيق أصلي بالنسبة إلى مستندات معينة حتى لا يتم فقد المحتوى المهم ، مثل ملاحظات المتحدث في العروض التقديمية أو تتبع التغييرات والتعليقات في مستندات معالجة الكلمات.

يمكن أن تكون المعلومات الإضافية في هذه المستندات مفيدة جدًا أيضًا في صياغة استراتيجية مراجعة المستندات والأدلة

الرقمية مما يسمح لشركة المحاماة والعميل لاكتساب فهم أشمل للحقائق في وقت مبكر من عملية الاكتشاف.

ثالثا : تحديد "المستندات"

من المهم أيضًا تحديد جميع أنواع البيانات المطلوبة حيثران الفشل فيعرض كل فئات "المستندات" المطلوبة بشكل فردي يمكن أن يؤدي إلى إغفال مصادر البيانات الرئيسية والمعلومات الهامة فمن المحتمل أن تكون هناك بيانات غير عادية ، مثل الدردشات والنصوص ومحركات الأقراص المشتركة والبريد الصوتي والتسجيلات الهاتفية.

يضمن طلب هذه الأنواع من المستندات في طلبات الاكتشاف أن يحصل العميل على الحقائق والاتصالات بشكل أساسي لبناء القضية ، لا سيما في الصناعات المعروفة بالاعتماد على هذه الأشكال من الاتصالات.

عند التفكير في أنواع المستندات المطلوب تقديمها كدليل رقمى بالتقاضى، من المهم أن تضع في اعتبارك أنه سيُطلب منك أيضًا على الأرجح إنتاج هذه الأنواع من المستندات أيضًا .إذا اعتقد أحد الأطراف أن العبء سيكون أكبر بكثير على عاتق الطرف الآخر لمراجعة وإنتاج فئة

---

[1] راجع فى ذلك :

خمس طرق لاستعادة التحكم في مستنداتك بعمليات الأعمال المكثفة:

https://www.lawtechnologytoday.org/2020/02/5-ways-to-retake-control-of-your-document-intensive-business-processes

معينة من المستندات ، وهذا العبء لا يفوقه المنفعة المحتملة لتلقي إنتاج الطرف الآخر لنفس البيانات ، لذا يجب إجراء دراسة متأنية من جانب أطراف الدعوى المعنيين بالتفاصيل الأخرى للتقاضي المطروح للتأكد من أنهم يركزون على أنواع المستندات التي من المرجح أن تحتوي على المعلومات المطلوبة مما يسمح بمراجعة مبسطة وفعالة لـ ESI وتطوير فهم كامل للحقائق والقضايا التي تنطوي عليها القضية.

رابعا : كيف تستخدم شركات قانونية تقنية E – discovery لصالحها[1]

التكنولوجيا تمكن من تنفيذ المهمة بشكل أكثر كفاءة ، و نظرًا لأن عددًا قليلاً جدًا من القضايا المدنية يذهب إلى المحاكمة ، فإن معظم التقنيات القانونية تركز على جمع المستندات ومعالجتها ومراجعتها ، ولكن حتى إذا لم تنتهي القضية في نهاية المطاف في قاعة المحكمة ، فلا يزال يتعين على المحامين إعداد استراتيجية للقضية وربما تقديم أدلة في الوساطة أو التحكيم ، ويمكن للفريق القانوني التركيز على المزيد من القضايا الموضوعية والوصول إلى جوهر القضية ، و ليس سراً أن المحامين ليسوا خبراء في التكنولوجيا ، لذلك قد يكون الأمر محبطًا عندما يتم تقديمهم ببرنامج يستغرق الكثير من الوقت للتعلم، **ونظرًا لأن كل حالة لها تحدياتها الفريدة الخاصة بها ، فإن التكنولوجيا سهلة الاستخدام يمكنها فقط أن تقدم العديد من الحلول من شريك تقني ذو خبرة كبيرة .**

[1] راجع فى ذلك:

https://www.lawtechnologytoday.org/2018/05/six-questions-you-must-ask-before-buying-e-discovery-software

https://www.lawtechnologytoday.org/2019/04/e-discovery-using-agile

المطلب الثالث

تحديات الاكتشاف الإلكترونى

كشفت دراسة حديثة أجرتها شركة تأمين ضد الممارسات الخاطئة أن ٪22من مكاتب المحاماة كانت ضحية للهجمات الرقمية .كان الضحايا أسماء أكبر في هذا المجال مما قد تتوقعه ، لكن الشركات الأصغر ليست مستثناة بأي حال من الأحوال .على سبيل المثال ، وجدت نقابة المحامين الأمريكية مؤخرًا أن هذا الرقم كان 35٪ في مكاتب المحاماة التي تضم 10–49 محامًا – مما يعني أن أكثر من ثلث مكاتب المحاماة الصغيرة قد تم اختراقها[1].

ومع ذلك ، بعيدًا عن كونه مسؤولية ، تفيد تقارير منظمات المجتمع المدني أن الذكاء الاصطناعي يوفر دعمًا إضافيًا في مكافحة التهديد المستمر للهجمات الرقمية .تسمح خوارزميات التعلم الذاتي المدمجة في تقنية الذكاء الاصطناعي بفهم التهديدات المحتملة والتنبؤ بها بشكل أفضل بطرق لا يستطيع البشر في كثير من الأحيان توقعها. في الواقع ، و يتسبب تطبيق الذكاء الاصطناعي في انخفاض مخاطر الأمن السيبراني.

1/ حاجة المستخدمين إلى المعلومات : و هي أحدى التحديات الأساسية التي تواجه عملية تطوير النظم والاحول بها الى الرقمية ، وقد أثبتت التجربة أن النظم الرقمية الناجحة هى التى يتم تطويرها إما على يد أو بمساعدة متخصصين ومبرجين ، حيث يوفر التقارب بين مطوري تلك النظم وبين المتخصصين فهما أعمق فيما يتعلق بطبيعة وخصائص المعلومات وكيفية استخدامها .

2/ سهولة الإستخدام : يجب على مطوري النظم أخذ عدة نقاط في الإعتبار أهمها طبيعة القانونين وحاجاتهم والفرق بينهم وبين محترفي العمل فى مجال تكنولوجيا المعلومات وأمن الشبكات .

3/ المعايير : فهي تساعد على زيادة الدقة والتكامل بين مختلف المؤسسات و تقلل من الأخطاء والتكاليف وترفع من قيمة البحث العلمي وتزيد من تكامل جهود التطوير واستثماراته .

[1] المرجع السابق.

4/التحديات الاجتماعية والقانونية : وهي تحديات تتعلق بمدى خصوصية وأمن المعلومات الرقمية، فكلما زادت سهولة الوصول إلى تلك المعلومات زادت أهمية إنشاء المزيد من قواعد ا لأمن والخصوصية التي تحكم عملية استخدام المعلومات وحق الإطلاع عليها .

5/**التكاليف مقابل المميزات** : وهي أهم التحديات الإقتصادية أمام صناعة نظم السجلات الرقمية، فكلما زادت الخواص والمميزات المطلوبة زادت في المقابل تكاليف إنتاجها وتوفيرها، ومن الضروري أن يتم الوصول إلى توازن مناسب بينهما[1] .

سابعا :أمن المعلومات وخصوصيتها[2]

على الرغم من أنه كثيرا ما يستخدم مصطلحا «الخصوصية» و «الأمن» بالتبادل، فإنهما تخصصان مختلفان؛ فأمن المعلومات وخصوصيتها هما تخصصان متميزان مرتبطان معا. ومن أجل الحماية المناسبة للخصوصية، تدعو الحاجة إلى آليات أمنية سليمة. ونظرا لحساسية المعلومات الشخصية التي يتم جمعها، واستخدامها، ومشاركتها في بيئة العمل القانونى، فمن المهم تحديد وتنفيذ الآليات الأمنية المناسبة التي من شأنها حماية البيانات وخصوصية الأفراد[3].

---

[1] https://linkitsys.com/ar/أمن البيانات الصحية في /ملف-المريض-السجل-الطبى-للمريض الأنترنت السحابي

[2] Osama Ahmed Attalla , Is The Legal Protection Of Digital Privacy Enough In Egypt" ? Protection Of Digital Data Privacy ", A Paper Submitted For The Conference Of Cyber Crimes , National Institute Of Intellectual Property April 2020 .

[3] راجع فى ذلك :

- http://www.alkhaleej.ae/alkhaleej/page/aaf7afa4-f9ac-4974-ab6e-cdb1ab5102b8#sthash.jTiWe8R0.dpuf
- http://www.alkhaleej.ae/alkhaleej/page/aaf7afa4-f9ac-4974-ab6e-cdb1ab5102b8
- https://ar.wikipedia.org/wiki/قانون_خصوصية_المعلومات
- https://www.consumersinternational.org/news-resources/news/arabic-news/blog-will-gdpr-be-the-global-standard-for-data-protection-arabic/ للائحة العامة لحماية البيانات: هل ستكون المعيار العالمي لحماية البيانات؟

ويجب تحديد متطلبات الأمن والخصوصية واختيار وتنفيذ الضوابط اللازمة خلال مراحل دورة تطوير النظام، وتحديث حماية الأمن والخصوصية حسب الحاجة. ومن المهم أيضا أن يتعاون الأفراد في منظمات أمن المعلومات والخصوصية لإدارة المخاطر الأمنية وحماية الخصوصية.

1 : ما الفرق بين الأمان والخصوصية؟[1]

في هذه الحقبة الرقمية التي تعتمد على التكنولوجيا يجب أن يكون الأمان والخصوصية من المطالب الرئيسية . حيث أصبح كل شيءٍ مرتبطًا ببعضه البعض ويمكن الوصول إليه بسهولة، فأغلب بياناتنا ومعلوماتنا الشخصية متاحة للقرصنة والتهديدات الأمنية، لذلك أصبح الجميع بحاجة للحماية والخصوصية ولاسيما الأشخاص الذين يعملون في مجالات الاتصالات. لكن معظمنا لا يدري ما هو الفرق بين الأمان والخصوصية.

ولسوء الحظ أصبحت الخروقات الأمنية شائعة جدًا، فوفقًا لتقرير جرائم الإنترنت لعام 2017 تمت سرقة أكثر من مليار سجل شخصي، وفي الولايات المتحدة وحدها أكثر من 100 مليون أميركي سُرقت سجلاتهم الطبية في عام 2016 ، وإن دلت هذه الإحصائيات على شيءٍ فإنها تدل على الحاجة الملحة لتعزيز الأمان والخصوصية[2]. وقبل الخوض في مسألة الفرق بين الأمان والخصوصية لا بد من تعريف كل منهما على حدى:

- **الأمان** :حالة تشير إلى الحرية الشخصية من القوى الخارجية والتحرر من الأخطاء المحتملة والتهديدات. ومثل نظام الأمان المنزلي الذي يحمي أسرتكم، فأمن البيانات يحمي البيانات والمعلومات الشخصية من خلال حمايته لكلمات مروركم ومستنداتكم. وكمثال عن الأمان البرامج المضادة للفيروسات على حاسوبك الشخصي التي تحمي جهازك وتجعل ملفاتك آمنة. ومع تطور التكنولوجيا وُضعت إجراءات صارمة وتدابير

[1] المهندس/ سعيد عطا الله, ما الفرق بين الأمان والخصوصية , مقال منشور بتاريخ :2020/5/14 على موقع :

https://www.arageek.com/l/ما-الفرق-بين-الأمان-والخصوصية/

[2] HIV.gov، The Difference between Security and Privacy and Why It Matters to Your Program، من موقع: www.hiv.gov، 2019-3-7 اطّلع عليه بتاريخ

لحماية البيانات الرقمية من الوصول غير المصرح به وحماية هذه البيانات من قراصنة الإنترنت والمجرمين الرقميين، وتحاول جميع التدابير الأمنية معالجة هدف واحدٍ من **أهداف الأمان وهي:** حماية السرية والحفاظ على سلامة أصول المعلومات وتعزيز توافر البيانات والمعلومات.

- **الخصوصية** :هي حق الشخص بالتحرر من الأعين المتطفلة ، وهي إحدى المبادئ الأساسية للكرامة الانسانية وتتضمن السرية وحماية المعلومات الحساسة كمعلومات التعريف الشخصية[1] ،وبالتالي من المستحيل تنفيذ برنامج خصوصية من دون وجود برنامجٍ أمني [2].

وبالرغم من التشابه بين المصطلحين والترابط الشائك بينهما، إلا أن الأمان هو حالة الحرية الشخصية والتحرر من التهديدات المحتملة، أما الخصوصية هي التحرر من الاهتمام غير المرغوب فيه والتطفل على الخصوصيات. ويتمثل الفرق بين الخصوصية والامان فى كلاً من :

- **الأهداف** :أهداف الأمان السرية والنزاهة والتوافر وحماية معلوماتك وبياناتك السرية من الوصول غير المسموح به. أما الخصوصية تشير إلى حقوق الأفراد والمؤسسات فيما يتعلق بالمعلومات الشخصية.
- **البرامج** :برنامج الأمن يشير إلى مجموعة من البروتوكولات واللوائح الموضوعة لجميع المعلومات السرية والموارد التي تجمعها المؤسسة وتمتلكها، وتركز على البيانات والمعلومات بدلًا من المعلومات الشخصية للأفراد. أما برنامج الخصوصية يركز على حماية المعلومات الشخصية فقط مثل تسجيل الدخول وكلمات المرور.

---

[1] للمزيد حول معنى الخصوصية راجع فى ذلك :

Osama Ahmed Attalla , Is The Legal Protection Of Digital Privacy Enough In Egypt" ? Protection Of Digital Data Privacy ", A Paper Submitted For The Conference Of Cyber Crimes , National Institute Of Intellectual Property April 2020.

[2] What's the Difference Between Privacy and Security?، من موقع: www.globalsign.com، اطّلع عليه بتاريخ 7-3-2019

- **المبادئ** :مبادئ الأمان تشمل حماية السرية والحفاظ على سلامة أصول المعلومات وتعزيز توافر البيانات والمعلومات. أما مبادئ الخصوصية فتحدد حقوق الأفراد والمنظمات فيما يتعلق بالمعلومات الشخصية.
- **الترابط والاعتماد بين المصطلحين** :يمكن تحقيق الأمان دون خصوصيةٍ، ولكن لايمكن تحقيق خصوصية دون أمان[1] .

تستند التشريعات التي تدافع عن الخصوصية على تعريفها كقيمة هامة لدي أفراد المجتمع. ونظرا لحداثة موضوع الخصوصية الرقمية تختلف الأطر التشريعية من دولة لأخرى طبقا للمستجدات التي مرت بها كل دولة، وفلسفتها التشريعية، وكيفية تطبيقها للقوانين والتحولات التي يمر بها المجتمع ومقدرة كل دولة على تبني تعديل لقوانينها بناء على قضايا جديدة تكون خارج اطارها التشريعي.[2]

وتهتم قوانين الخصوصية بحماية وسائط نقل المعلومات إما عبر الإنترنت أو الهواتف أو حتي البريد، كما تتضمن الحفاظ على سرية المعلومات الخاصة للأفراد الموجودة في سجلاتهم مثل المعلومات المالية أو الصحية. كما يجب أن تضمن بياناتهم الخاصة التي يتم تداولها من خلال التصفح والتواصل على الإنترنت.

هذا ولقد نتج عن استخدام الإنترنت تحديات مختلفة لموضوع حماية الخصوصية، وتختلف أنواع القوانين المختصة بالخصوصية في الفضاء الرقمي فهي تتراوح بين حماية البريد الرقمي، وفرض قيود على نشر بيانات التواصل الاجتماعي، ومتابعة نشاط متصفح الإنترنت والمخالفات للبيانات المحفوظة. وفيما يلي الأنواع المختلفة لقوانين الخصوصية الرقمية:

---

[1] Difference Between Security and Privacy من موقع: www.differencebetween.net، اطّلع عليه بتاريخ 7-3-2019

[2] https://sitcegypt.org/?p=1425/ تشريعات الخصوصية الرقمية

- **قانون حماية البيانات** :تفرض على الشركات المقدمة لخدمات الانترت والتي تقوم بتخزين معلومات رقمية لعملائها من نشر هذه المعلومات أو مشاركتها مع أطراف أخري دون إفادة من العميل.[1]
- **قانون مراقبة الإتصالات**:تُقيد مراقبة وسائل الإتصال بالإنترنت، والتي تكون في مجال العمل أو الموجودة في الأماكن العامة أو حتي في المنزل.
- **قانون الحماية من جرائم الإنترنت** :تمنع الاستيلاء على الهوية أو سرقة البريد الرقمي وكل ما يخص حماية البيانات الشخصية التي يشاركها الفرد أثناء استخدامه للانترنت.

2 : كيف يعمل الأمن والخصوصية معا ؟

هناك حاجة إلى تدابير أمنية لحماية خصوصية الأفراد. تُعرف التقنيات والأدوات التي تدعم الخصوصية بالتقنيات المعززة للخصوصية، وغالبا ما تتكون من تقنيات أمنية يحمي استخدامها خصوصية الأفراد. ويمكن استخدام التقنيات المعززة للخصوصية لأداء وظائف مثل تمكين الوصول إلى البيانات واستخدامها على نحو ملائم داخليا، ومنع الإفصاح غير الملائم عن البيانات خارجيا. ومع ذلك، فمثلما تستخدم الآليات الأمنية للمساعدة على جهود الخصوصية، فإن بعض تدابير الخصوصية تساعد أيضا في الجهود الأمنية.

[1]راجع فى ذلك:

www.dlapiperdataprotection.com., Data Protection Laws of the World

المطلب الرابع

التخطيط الناجح الاكتشاف الإلكترونى

يتمثل أحد الأهداف الرئيسية لـ E – discovery في تحديد وإنتاج المستندات غير المميزة التي تستجيب لأمر استدعاء أو طلب الكشف عن المستندات أو احتياجات التحقيق ، وكذلك حجب المستندات غير المستجيبة والتي تتمتع بامتيازات قانونية ، **ويمكن أن تؤدي ESI التي تم جمعها لانتهاك مبادئ الطب الشرعي كما** يمكن ان تؤدى معالجتها وتحليلها بشكل غير صحيح إلى إهدار تكاليف ووقت كبير. لذلك اصبح من الضرورى التخطيط لإنجاح عملية الاكتشاف الإلكترونى وهو ما سنعرض له على النحو التالى:

أولا :التقنيات والأدوات

عند البدء يجب جمع ESI ومعالجته واستضافته في قاعدة بيانات جيدة التنظيم،كما يجب تحويل النسخ الورقية إلى ESI عن طريق المسح الضوئي وجعلها قابلة للبحث عن النص باستخدام برنامج التعرف الضوئي على الأحرف ، و تتضمن المعالجة تجميع وتوحيد أنواع متنوعة من ESI مثل رسائل البريد الرقمي ورسائل الدردشة ومستندات Word وملفات PDF والملفات الصوتية ، مما يجعلها بيانات منظمة وقابلة للبحث كما يمكن لأدوات المعالجة أيضًا استبعاد الملفات المكررة والتالفة والملفات التي تحتوي على محتوى تم إنشاؤه بواسطة الكمبيوتر بعد إنشاء مجموعة من المستندات للمراجعة اليدوية ، ولكن قبل أن تبدأ المراجعة فعليًا ، يمكن تقسيم المجموعة ، وتحديد الأولويات.

ثانيا: أتمتة وتسريع المراجعة باستخدامAnalytics

التقنيات والأدوات التقليدية لها حدودها عند البحث عن طريق الكلمات الرئيسية ، ويقوم المراجعون بشكل أساسي بتخمين الكلمات التي استخدمها مؤلفو المستندات ، ولكن سوف تؤدي عمليات البحث عن الكلمات الرئيسية هذه إلى نتائج غير شاملة (على سبيل المثال ، تم حذف المستندات لأن المراجع ليس على دراية ببعض الاختلافات والأشكال الإقليمية التي اعتمدها المؤلف ، وقد تكون هناك أخطاء إملائية) ونتائج شاملة (على سبيل المثال ، اختيار الكلمات الرئيسية غير المستجيبة) المستندات لأن الكلمات قد تم استخدامها في سياقات من المحتمل ألا

تكون ذات صلة .(على سبيل المثال ، يمكن أن تتعلق المستندات التي تحتوي على كلمة "تفاحة" بكل من الشركة والفاكهة التي تحمل الاسم نفسه ، ولكن الشركة فقط قد تكون هي المستجيبة للقضية) ، ومن الممكن لأحدث برامج التحليلات أن تزيد من دقة نتائج البحث وتقليل الإيجابيات والسلبيات الخاطئة كما يمكن للبرنامج تجميع المستندات التي تم تحديدها ذاتيًا ، وتصنيفها ، ووضع تصور لها من خلال أنماط متكررة معينة من الكلمات الواردة فيها ، و توفر عدة أنواع من برامج E – discovery المتقدمة إمكانات" **الترميز التنبئي**[1]" ، والتي أقرتها المحاكم الأسترالية والإنجليزية والأيرلندية والأمريكية كأدوات مناسبة في الاكتشافات التي تتضمن أحجامًا كبيرة من ESI باستخدام خوارزميات التعلم الآلي ، بناءً على إطار عمل التحليلات ، يحدد برنامج الترميز التنبئي المستندات التي تستجيب ويرتيبها حسب الأولوية

من خلال مزيج من تقنيات E – discovery التقليدية والمتقدمة ، يمكن إجراء مراجعة وإنتاج ESIعلى نطاق واسع ، مع ضمان جودة واتساق التحليل ، وتقليل مخاطر الخطأ ، وإدارة التكاليف والجداول الزمنية بكفاءة.[2]

---

[1]الترميز التنبئي للمبتدئين: الإكتشاف الإلكترونى في قاعة المحكمة

— https://www.lawtechnologytoday.org/2014/10/predictive-coding-for-rookies-e-discovery-in-the-courtroom

[2]راجع فى ذلك :

مساعد افتراضي مزايا وجود مساعد افتراضي في فريقك

— https://www.lawtechnologytoday.org/2021/05/advantages-of-having-a-virtual-assistant-in-your-team

الابتكار الذي يحركه العميل: مستقبل التكنولوجيا القانونية

— https://www.lawtechnologytoday.org/2019/07/client-driven-innovation-the-future-of-legal-technology

مدراء دعم التقاضي Upskill لإضافة قيمة على مستوى الشركة

— https://www.lawtechnologytoday.org/2019/06/upskill-litigation-support-managers-to-add-value-firm-wide

التنوع في القانون: هل يمكن أن يساعد تعليم التكنولوجيا القانونية في تحريك الإبرة؟

ثالثا : التخطيط للاكتشاف الرقمي[1]

يعد الاكتشاف الإلكترونى عملية معقدة تتطلب نهجًا متعدد التخصصات للتنفيذ والإدارة بنجاح، و يجب على المؤسسات خاصة الرعاية الصحية إكمال الأنشطة العشرة التالية للتحضير للاكتشاف الرقمي:

- إنشاء فريق استجابة للتحقيق والتقاضي مع من ينوب عنه من الإدارات القانونية و HIM و IT .
- مراجعة أو تطوير خطة إدارة المعلومات التنظيمية وتزويد المستشار القانوني بأي وجميع الخطط السابقة التي وضعتها الادارة او الهيئة.
- تحديد مالكي البيانات أو المشرفين داخل الادارة او الهيئة.
- مراجعة و تطوير جدول الاحتفاظ بسجلات الادارة.
- إجراء تقييم شامل للمواقع والنماذج والاستخدام التجاري والقانوني لجميع الأنظمة القديمة ووسائط النسخ الاحتياطي والبيانات المعزولة الموجودة.
- مراجعة و تطوير السياسات التنظيمية المتعلقة بالاكتشاف الإلكترونى.
- مراجعة و تطوير السياسة التنظيمية لإدارة البريد الرقمي.
- تطوير منهجية راسخة لتحديد أعباء وتكاليف إنتاج المعلومات المخزنة رقميًا.
- حدد الشخص (الأشخاص) المعين المسؤول عن إنشاء عملية احتجاز قانوني داخل الادارة او الهيئة.

— https://www.lawtechnologytoday.org/2019/06/can-legal-tech-education-help-move-the-needle

التحول الرقمي: الآثار الرئيسية لخدمات وعروض تكنولوجيا شركة المحاماة

— https://www.lawtechnologytoday.org/2019/05/digital-transformation-key-implications-for-law-firm-technology-services-and-offerings

[1] AHIMA. "E- Discovery Litigation and Regulatory Investigation Response Planning: Crucial Components of Your Organization's Information and Data Governance Processes." Journal of AHIMA 84, no.11 (November-December 2013): expanded web version.

- إنشاء برنامج تنظيمي لتثقيف وتدريب جميع الإدارة والموظفين على الامتثال[1] للاكتشاف الرقمي .

رابعا : تطوير السياسة والإجراءات التنظيمية

الخطوة التالية في التقاضي وتخطيط الاستجابة التنظيمية هي تطوير أو تحديث السياسات والإجراءات التنظيمية المتعلقة بالاكتشاف الإلكترونى لذا يجب أن يكون لدى المنظمات السياسة والإجراءات التالية:

****التحضير لمؤتمر ما قبل المحاكمة[2]:**

الهدف من هذه السياسة هو التأكد من أن الادارة او الهيئة تستعد بشكل كافٍ لمؤتمر ما قبل المحاكمة.

****الحفظ والتحفظ القانوني للسجلات والمعلومات[3]:**

---

[1] Dimick, Chris. "E-Discovery: Preparing for the Coming Rise in Electronic Discovery Requests." Journal of AHIMA 78, no. 5 (May 2007): 24-29. Federal Rules of Civil Procedure http://www.law.cornell.edu/rules/frcp

[2] راجع فى ذلك :

ثلاثة أسئلة رئيسية يجب طرحها قبل التجميع عن بُعد:

- https://www.lawtechnologytoday.org/2020/12/three-key-questions-to-ask-before-collecting-remotely/

[3] راجع فى ذلك :

- http.//www.healthvault.com
- http://www.alkhaleej.ae/alkhaleej/page/aaf7afa4-f9ac-4974-ab6e-cdb1ab5102b8#sthash.jTiWe8R0.dpuf
- https://aitnews.com/2018/05/27/اللائحة-العامة-لحماية-البيانات-gdpr/
- https://ar.wikipedia.org/wiki/قانون_خصوصية_المعلومات
- https://hi-in-ksa.com/2015/12/20/قواعد-بياناتا-ومجلات-علمية-في-المعلوم/
- HTTPS://ME.KASPERSKY.COM/ENTERPRISE-SECURITY/HEALTHCARE

تحدد هذه السياسة عملية حفظ السجلات الورقية والرقمية والمعلومات ذات الصلة للحماية من سرقة الأدلة.[1]

****الاحتفاظ بالمعلومات والسجلات الورقية والرقمية وتخزينها وإتلافها[2]:**

---

[1]راجع فى ذلك :

هل يمكن للتقدم التكنولوجي أن يؤجج أزمة سوء الممارسة الطبية؟

— https://www.lawtechnologytoday.org/2021/05/can-tech-advances-fuel-a-medical-malpractice-crisis

[2]راجع فى ذلك : د.أمل فوزى أحمد ، بحث بعنوان " التحديات القانونية لخصوصية وأمن المعلومات الطبية الرقمية" منشور في المؤتمر الدولي الافتراضي الأول تحت عنوان : " دور المؤسسات في تحقيق التنمية المستدامة في ظل الاوبئة العالمية ، يومي 16 و15 يوليو 2020 ، مرجع سابق

- https://mobile.emirates.com/MobileTermsConditions/jo/arabic/what_sensitive_personal_data_might_you_require_or_hold.xhtml?lang=ar_JO
- HTTPS://TAQADOM.ASPDKW.COM / أمن-المعلومات-الصحية/, تاريخ احر دخول: 28/6/2020
- https://www.arageek.com/l/ما-الفرق-بين-الأمان-والخصوصية
- https://www.consumersinternational.org/news-resources/news/arabic-news/blog-will-gdpr-be-the-global-standard-for-data-protection-arabic/ للائحة العامة لحماية البيانات: هل ستكون المعيار العالمي لحماية البيانات؟
- https://www.ehealthsa.com/archives/2261
- https://www.lita-lb.org/archive/51-dossier-médical-electronique.html) تاريخ اخر دخول : 29/6/2020)"
- https://www.lita-lb.org/archive/51-dossier-médical-electronique.html
- https://www.salamatech.org/الخصوصية-من-منظور-حقوق-الإنسان/
- www.globalsign.com، اطّلع عليه بتاريخ 7-3-2019
- www.differencebetween.net، اطّلع عليه بتاريخ 7-3-2019
- www.hiv.gov، اطّلع عليه بتاريخ 7-3-2019
- https://linkitsys.com/ar/ ملف-المريض-السجل-الطبى-للمريض/ أمن البيانات الصحية في الأنترنت السحابي
- https://sitcegypt.org/?p=1425 /تشريعات الخصوصية الرقمية

تحدد هذه السياسة الشروط والفترات الزمنية التي سيتم فيها تخزين السجلات الورقية والرقمية والاحتفاظ بها وإتلافها بعد أن لم تعد ذات جدوى ، ويجب أن يرافق الجدول الزمني للاحتفاظ بسجلات الادارة وتدميرها هذه السياسة لتوفير محاسبة كاملة ودقيقة لجميع مسؤولي السجلات ذات الصلة داخل الادارة او الهيئة.

****إنتاج والكشف عن المعلومات والسجلات الصحية الرقمية[1]:**

تحدد هذه السياسة الخطوات في عملية الإفصاح عن السجلات الرقمية والمعلوماتية المتعلقة بإجراء قانونى ، ويتم إدارة العديد من هذه الإجراءات من خلال إدارة المعلومات.

خامسا : تطوير نظام للمراقبة والتقييم المستمر[2]

- https://taqadom.aspdkw.com/أمن-المعلومات-الصحية/
- https://hi-in-ksa.com/2013/07/08/

[1]راجع فى ذلك :

المهندس/ سعيد عطا الله ,ما الفرق بين الأمان والخصوصية, مقال منشور بتاريخ :14/5/2020 على موقع:

_ https://www.arageek.com/l/ما-الفرق-بين-الأمان-والخصوصية

معايير جديدة تضيفها منظمة "HIMSS" تركز فيها على أمن المعلومات والتصوير الطبي مقال منشور 25 أبريل، 2017 على موقع:

_ https://www.ehealthsa.com/archives/2261

د. إيهاب عبد الرحيم علي , أمن المعلومات الصحية مقال منشور على:

_ HTTPS://ME.KASPERSKY.COM/ENTERPRISE-SECURITY/HEALTHCARE

أمن-المعلومات-الصحية , مقال منشور على:

_ HTTPS://TAQADOM.ASPDKW.COM / أمن-المعلومات-الصحية/,تاريخ احر دخول : 28/6/2020

_ https://www.lita-lb.org/archive/51-dossier-médical-electronique.html(تاريخ اخر دخول : 29/6/2020 ")

[2]راجع فى ذلك :

TechReport 2020: التقاضي وتقييم الأثر

_ https://www.lawtechnologytoday.org/2020/11/techreport-2020-litigation-tar

_ ABBYY

حلول الذكاء الرقمي لتحويل العمليات القانونية في جمعية المحامين الأمريكية2020 TECHSHOW

تمتد مسؤوليات فريق الاكتشاف إلى تقييم فعالية سياسات وإجراءات الادارة او الهيئة بعد التنفيذ ،ويشمل ذلك تطوير ومراجعة تدريب الموظفين على الاكتشاف الإلكترونى ومراجعة مواد التدريب السنوية وإنشاء عملية تدقيق والمراقبة المستمرة لإنشاء قواعد البيانات وأدارة المعلومات والأمن الرقمى لتقييم الالتزام بسياسات الاكتشاف الإلكترونى في جميع أنحاء الادارة او الهيئة.

_ https://www.lawtechnologytoday.org/2020/02/abbyy-to-showcase-digital-intelligence-solutions-to-transform-legal-operations-at-the-american-bar-association-techshow-2020/

المطلب الخامس

الذكاء الاصطناعي والاكتشاف الإلكترونى[1]

لقد توقع البعض في المجال القانوني أن الذكاء الاصطناعي ("AI") سيلعب دورًا مؤثرًا بشكل متزايد في تقديم الخدمات القانونية وسيجلب فهمًا أكبر لكيفية تعزيز{ تحليلات البيانات} والذكاء الاصطناعي .

اولا : تعريف الذكاء الاصطناعي[2]

ببساطة ، الذكاء الاصطناعي هو استخدام "التكنولوجيا لأتمتة المهام التي تتطلب عادةً ذكاءً بشريًا " تتضمن هذه المهام القدرات البشرية على التفكير والتحليل والتعميم وحل المشكلات والتعلم ، ويتُصنف أنظمة الذكاء الاصطناعي بأنها "قوية" أو "ضعيفة" بناءً على درجة قدرتها على أداء القدرات البشرية ، ويساعد هذا التمييز في تحديد نطاق قدرات أنظمة الذكاء الاصطناعي الحالية ، على الرغم من أن هذه القدرات تقع عبر نطاق وليس ضمن فئات متميزة .

يكون الذكاء الاصطناعي "قويًا" حقًا عندما يمكنه على الأقل "أداء أي مهمة فكرية يستطيع الإنسان فعلها بنجاح" ، إن لم يكن لديه أيضًا القدرة على تجربة الوعي وفهم مفاهيم مثل اللغة.

---

[1] راجع فى ذلك :

_ https://www.lawtechnologytoday.org/2021/02/using-artificial-intelligence-to-improve-law-firm-performance

[2] راجع فى ذلك :

“Intellectual property and artificial intelligence Reality & the Future”, BISKRA UNIVERSITY – FACULTY OF LAW AND POLITICAL SCIENCES Laboratory impact of jurisprudence on the dynamics of legislation, Jurisprudence Journal –. Vol 35 – (Special Issue – S N 42) – 19 January 2021.

وعلى الرغم من "ضعف" أنظمة الذكاء الاصطناعي مثل ، AlphaGo يمكن للذكاء الاصطناعي الضعيف أداء مجموعة متنوعة من المهام البشرية[1] .

ثانيا : فائدة الذكاء الاصطناعي في الصناعة القانونية

على وجه التحديد لاستخدامه في الصناعة القانونية ، يمكن تعريف الذكاء الاصطناعي على أنه أتمتة المهام عبر البرامج لتحقيق نفس النتيجة "كما لو أن ممارسًا قانونيًا قد قام بالعمل كما "يمكن تجميع المهام القانونية التي تؤديها أنظمة الذكاء الاصطناعي حاليًا في واحد من ثلاثة مجالات: تحليل المستندات[2] ، والبحث القانوني ، وأتمتة المهام .

ثالثا :حدود الذكاء الاصطناعي

تطوير واستخدام الذكاء الاصطناعي محدودان فيما يتعلق بالبيانات والخوارزميات والتنفيذ وحيث تلعب البيانات دورًا مركزيًا في أنظمة الذكاء الاصطناعي كمواد تدريبية لتطوير خوارزميات الذكاء الاصطناعي ومواد الإدخال للاستخدام الفعلي للذكاء الاصطناعي . لكن تطوير واستخدام خوارزميات الذكاء الاصطناعي مقيد بنقص البيانات التي يسهل الوصول إليها والتحليل" فمكاتب المحاماة" غنية بالوثائق وفقيرة للبيانات "والبيانات العامة مثل الآراء القضائية إما أنها غير متوفرة أو متنوعة في الشكل بحيث يصعب استخدامها بفعالية .علاوة على ذلك ، يمكن أن تؤدي

---

[1]تستخدم الشركات الذكاء الاصطناعي الضعيف للتطبيقات التي تتراوح من تحديد الأسعار إلى السيارات ذاتية القيادة والموافقة على القروض إلى تشغيل روبوت المستودعات استخدم الباحثون الذكاء الاصطناعي الضعيف لتحديد سرطان الثدي وتفشي الفيروسات المعدية مثل "فيروس ووهان" يستخدم المستهلكون ذكاءً اصطناعيًا ضعيفًا عندما يجرون بحثًا علىGoogle أو Bingيتحدثون باستخدام ذكاء اصطناعي ضعيف عندما يسألون أليكسا أو بيكسبي أو كورتانا أو مساعدGoogle أو Siriيستخدم المحامون الذكاء الاصطناعي الضعيف لمجموعة متنوعة من التطبيقات أيضًا.

[2]تشمل الفئة الواسعة لتحليل المستندات تحليل العقود ومراجعة المستندات والإكتشاف الإلكترونى والعناية الواجبة تقدم الشركات القديمة والجديدة أدوات تحليل المستندات المدعومة بالذكاء الاصطناعي على سبيل المثال استخدمتJPMorgan برنامجها الخاص بعنوان Contract Intelligence ، الملقب بـ "COIN" ، لتقليل وقت مراجعة العقد السنوي بمقدار 360.000 ساعة، و تقدم الشركات الأحدث مثل Kira Systems و eBrevia كما ازداد استخدام الذكاء الاصطناعي في الإكتشاف الإلكترونى بشكل كبير نظرًا للكفاءات التي يوفرها.

مجموعات البيانات ذات الجودة الرديئة أو المعيبة إلى قيام أنظمة الذكاء الاصطناعي بإخراج نتائج متحيزة فقد يكون لمجموعات البيانات جودة رديئة أو عيوب لعدة أسباب ، وقد تؤدي تقنيات جمع البيانات أو إعدادها إلى تحيزات إحصائية في مجموعة البيانات مثل العينات غير التمثيلية (انحياز الاختيار) .قد يتم التلاعب بمجموعات البيانات أو إتلافها عمدًا للحصول على تحليلات غير عادلة .بالإضافة إلى مشكلات جودة البيانات ، وقد تنشأ أيضًا مخاوف كبيرة بشأن خصوصية البيانات[1] والأمن السيبراني[2] مع استخدام كميات هائلة من البيانات بواسطة أنظمة الذكاء الاصطناعي [3].

---

[1]راجع فى ذلك :

_ Osama Ahmed Attalla, Is The Legal Protection Of Digital Privacy Enough In Egypt''? Protection Of Digital Data Privacy ", A Paper Submitted For The Conference Of Cyber Crimes, National Institute Of Intellectual Property April 2020

_ بحث بعنوان " معالجات تشريعية لضبط الحقوق والحريات فى البيئة الرقمية" المؤتمر العلمى السادس , القانون والشائعات ,كلية الحقوق ,جامعة طنطا ,23-24 ابريل 2019.

[2]راجع فى ذلك :

الأعمال الصغيرة: تدابير اختبار الأمن السيبراني:

_ https://www.lawtechnologytoday.org/2021/05/small-business-cyber-security-testing-measures

_ بحث بعنوان " الامن الانسانى فى ظل تحديات التحول الى الرقمية لمستقبل حقوق الانسان " ، الملتقى الدولى الموسوم " الأمن الإنسـاني في ظل التحديات العالمية المعاصرة " ، 9 و10 يناير 2021.

[3]راجع فى ذلك :

اتبع أفضل ممارسات أمان البريد الرقمي:

_ https://www.lawtechnologytoday.org/2021/05/working-from-home-7-cybersecurity-tips-to-protect-your-data

يجب على مستخدمي الذكاء الاصطناعي المحتملين إدراك أن النشر الفعال للتكنولوجيا قد يكون أصعب مما يتوقع فالتحدي الأكبر هو ببساطة جعل المستخدمين المحتملين يثقون بالتكنولوجيا [1].

هذا ويفترض الباحثون أن الذكاء الاصطناعي سيؤثر على الواجبات الأخلاقية للمحامين فيما يتعلق بالكفاءة التقنية ، والسرية ، والإشراف ، والتواصل مع العميل ، والحكم المستقل ، والممارسة غير المصرح بها للقانون ، والرسوم الزائدة ، وتضارب المصالح ، ووتيرة التطور السريع للذكاء الاصطناعي تجعل من تحديد حدود تلك الواجبات من جانب التشريعات مسألة ملحة.

رابعا :كيف ينبغي للمحامين التعامل مع صعود الذكاء الاصطناعي في تقديم الخدمات القانونية والتكيف معه؟[2]

---

[1]راجع فى ذلك :

مزايا وجود مساعد افتراضي في فريقك :

_ https://www.lawtechnologytoday.org/2021/05/advantages-of-having-a-virtual-assistant-in-your-team

الابتكار الذي يحركه العميل: مستقبل التكنولوجيا القانونية

_ https://www.lawtechnologytoday.org/2019/07/client-driven-innovation-the-future-of-legal-technology

مدراء دعم التقاضي Upskill لإضافة قيمة على مستوى الشركة

_ https://www.lawtechnologytoday.org/2019/06/upskill-litigation-support-managers-to-add-value-firm-wide

التنوع في القانون: هل يمكن أن يساعد تعليم التكنولوجيا القانونية في تحريك الإبرة؟

_ https://www.lawtechnologytoday.org/2019/06/can-legal-tech-education-help-move-the-needle

التحول الرقمي: الآثار الرئيسية لخدمات وعروض تكنولوجيا شركة المحاماة

_ https://www.lawtechnologytoday.org/2019/05/digital-transformation-key-implications-for-law-firm-technology-services-and-offerings

[2]راجع فى ذلك :

الذكاء الاصطناعي لديه القدرة على التأثير بشكل كبير على مهنة القانون ، و يخشى البعض أن يلحق الذكاء الاصطناعي الضرر بالمحامين وغيرهم من المهنيين القانونيين لأن التكنولوجيا تحل محل أجزاء على الأقل من وظائفهم وتقلل من فرص التدريب كما يتوقع آخرون أن الذكاء الاصطناعي سيساعد المحامين على تطوير ممارساتهم للتركيز على المهام ذات القيمة الأعلى والأدوار الجديدة أو فرص تقديم الخدمات . ولقد قدم الكثيرون نصائح عملية حول كيفية تكيف المحامين مع استخدام الذكاء الاصطناعي في الصناعة القانونية ، ولكن كيف يتعامل كل محام مع الذكاء الاصطناعي ويتكيف معه في السوق القانوني هو سؤال يجب أن يجيب عليه المحامى بنفسه.

إن تطور واستخدام الذكاء الاصطناعي (AI) آخذ في الارتفاع ولا يظهر أي علامات على التوقف في المستقبل القريب ، ومن المتوقع أن تزيد الإيرادات العالمية من تطبيقات المؤسسات التي تستخدم الذكاء الاصطناعي بنحو 30 مليار دولار بحلول عام 2025. مع هذا النمو الهائل ، ولحسن الحظ ، فإن المجال القانوني هو أرض خصبة لفوائد تكنولوجيا الذكاء الاصطناعي حيث يمكن الآن إنجاز المهام التي تستغرق وقتًا طويلاً باستخدام الأتمتة والتعلم الآلي في وقت أقل وبتكلفة أقل.

خامسا :الوضع الحالي لتكنولوجيا الذكاء الاصطناعي

الذكاء الاصطناعي هو أداة مفيدة يتم استخدامها على نطاق واسع في تطبيقات العالم الواقعي التي تتعلم إكمال المهام التي يقوم بها البشر عادة. حتى بالنسبة للعباقرة ، من غير الواقعي للمحامين الاحتفاظ بقائمة كاملة لكل ما يحتاجون إلى معرفته في رؤوسهم في جميع الأوقات .ومع ذلك ، فإن الوصول إلى كل جزء من البيانات ذات الصلة بشأن إجراء ونتائج مسألة سابقة يمكن أن يكون ميزة كبيرة في تحقيق نتائج إيجابية في مسائل مماثلة في المستقبل .هذا هو المكان الذي يأتي فيه الذكاء الاصطناعي.

_ https://www.lawtechnologytoday.org/2019/04/artificial-intelligence-will-change-e-discovery-in-the-next-three-years

"نظرًا لأن الذكاء الاصطناعي يمكنه الوصول إلى المزيد من البيانات ذات الصلة ، فإنه يمكن أن يكون أفضل من المحامين في التنبؤ بنتائج النزاعات والإجراءات القانونية ، وبالتالي مساعدة العملاء على اتخاذ القرارات .على سبيل المثال ، استخدمت شركة محاماة بلندن بيانات عن نتائج 600 قضية على مدى 12 شهرًا لإنشاء نموذج لجدوى حالات الإصابة الشخصية .في الواقع ، تم تدريب الذكاء الاصطناعي على 200 عام من سجلات المحكمة العليا ، وهو بالفعل أفضل من العديد من الخبراء البشريين في توقع قرارات.[1]

للذكاء الاصطناعي أيضًا العديد من التطبيقات الأخرى – الأكثر وضوحًا – التي يمكن لمكاتب المحاماة الاستفادة منها. بدلاً من قضاء ساعات العمل في إكمال المهام الشاقة والحذرة ، والتي يمكن للذكاء الاصطناعي القيام بها بكفاءة . فالذكاء الاصطناعي "ليس ظاهرة جديدة تمامًا ، والصناعة القانونية تستخدم الذكاء الاصطناعي في عملية اكتشاف التقاضي منذ ما يقرب من 10 سنوات."لقد شق الذكاء الاصطناعي طريقه بالفعل إلى مهنة القانون من خلال البحث القانوني ، ومراجعة العقود ، والإدارة ، ومراجعة الوثائق ، والتنبؤ بالنتائج القانونية ، وغير ذلك فمن المحتمل أن يكون ظهور الاكتشاف الإلكترونى هو أقرب مثال على استخدام الذكاء الاصطناعي في المهنة القانونية مع كل شيء منظم في شكل رقمي ، و يتيح الذكاء الاصطناعي للمتقاضين تنظيم المعلومات ذات الصلة وترابطها والبحث عنها بطرق أكثر فاعلية بكثير مما تسمح به المراجعة اليدوية للوثائق الورقية.

علاوة على ذلك ، وفقًا لـ Bloomberg Law ، فإن الذكاء الاصطناعي "يساعد الباحثين القانونيين على اكتشاف الوثائق التي لم يكن بإمكانهم العثور عليها سابقًا وتحديد أوجه التشابه بين آراء المحاكم بسهولة أكبر. هذا بالإضافة إلى القدرة على تحليل الملايين من نقاط البيانات القانونية ، بكفاءة كل ذلك بضغطة زر كما يمكن للذكاء الاصطناعي تزويدك بمعلومات لم تكن تعرف حتى للبحث عنها.

---

[1] راجع في ذلك :

استخدام الذكاء الاصطناعي لتحسين أداء شركة المحاماة:

- https://www.lawtechnologytoday.org/2021/02/using-artificial-intelligence-to-improve-law-firm-performance

المبحث الثاني

الأدلة الرقمية [1]

يحتل عنصر الإثبات مكانة مرموقة في كافة العلاقات والمجالات الشخصية والمدنية والتجارية، وهو الوسيلة الأساسية للحصول علي الحقوق وإلزام الآخرين بالوجبات. ومن الناحية العملية ليس للحق أية قيمة عندما يعجز صاحبه عن إثباته ، إذ أن إثبات الفعل المولّد للحق هو الذي يعطي هذا الحق فعاليته الكاملة .

والإثبات هو نظام قانوني[2] ، بحيث لا يُقبل من طرقه ووسائله إلا تلك التي حددها القانون. وقد اعتبر القانون أن بعض هذه الوسائل يتمتع بقوة ثبوتية كاملة لإثبات جميع التصرفات القانونية والوقائع المادية؛ مثل: السند الكتابي(الرسمي أو العادي) ، الإقرار ، اليمين الحاسمة والقرائن القانونية .

---

[1] راجع في ذلك : أحمد حمو، علاء عواد، ولاء عبد الله ، الأدلة الرقمية (الجوانب القانونية والتقنية) ، أوراق بحثية في القانون ومكافحة الفساد ، معهد الحقوق، جامعة بيرزيت، هيئة مكافحة الفساد ، فلسطين ، 2015 ، ص10 وما بعدها ، وراجع أيضا : ا .د / براء منذر كمال عبداللطيف ، د / ياسر عواد شعبان ، الأدلة الحديثة ودورها في الإثبات الجنائي، بحث مقدم للمؤتمر العلمي السنوي ، كلية الحقوق جامعة أسيوط ، بعنوان " العصر الرقمي" ، في الفترة من 12 إلي 13 إبريل 2016 ، ص 20 وما بعدها ، وراجع أيضا : ا .د / براء منذر كمال عبداللطيف ، ا .م .د / أمير حسن جاسم ، المستندات الرقمية وحجيتها في الإثبات ، بحث مقدم للمؤتمر العلمي السنوي ، كلية الحقوق ، جامعة أسيوط ، بعنوان " العصر الرقمي" ، في الفترة من 12 إلي 13 إبريل 2016 ، ص 4 وما بعدها ، وراجع أيضا :

- https://docplayer.net/13165153-Making-reliable-web-services-message-exchanges-secure-and-tamper-proof-alan-j-weissberger-data-communications-technology-aweissberger-sbcglobal.html (تاريخ آخر دخول علي الموقع 2020/9/22)
- https://docplayer.net/21648942-Second-amended-order-designating-all-cases-e-file-and-setting-forth-certain-requirements-in-e-file-cases.html (تاريخ آخر دخول علي الموقع 2020/9/22)

[2] راجع في ذلك : د/عبد التواب مبارك ، الدليل الرقمي أمام القاضي المدني ، دار النهضة العربية ، بدون سنة نشر ، ص 5 وما بعدها .

لكن دخول العالم في عصر الثورة الصناعية الرابعة ،**4.0** والتحول إلي الرقمية ، أدي إلي تغير مفهوم الإثبات تبعاً لإمكانية إنشاء الحقوق والالتزامات بطرق رقمية ، والاستغناء في غالبية الأحيان عن الكتابة الورقية.

ولم يعد بالإمكان سوي الاعتراف بهذا العالم الجديد الذي يقوم علي علم المعلوماتية والتكنولوجيا، وهو يعتمد أسلوباً غير ورقي ، مرئياً ومنقولاً عبر الشاشة الرقمية. وقد تم استبدال الملفات الورقية والمخطوطات بالأسطوانات الممغنطة والسندات الرقمية المحفوظة علي أسطوانات ضوئية رقمية أو علي أقراص ممغنطة ، وهي تنتقل من مكان إلي آخر بسهولة وسرعة خارقة من دون أية حاجة للورق.

ولقد أصبحت غالبية الالتزامات والعقود والمعاملات تقوم بالوسائل الرقمية ، تبعاً لما يوفره الإنترنت كوسيلة سهلة وفعالة ، ومتوافرة للعموم ، وتتيح الحصول علي المعلومات وحفظها وتبادلها ، من دون أن تعترضها الحدود الجغرافية.

- **الإشكاليات القانونية في الإثبات الرقمي[1] :**

إن أول ما يُطرح في موضوع الإثبات هو توفر السند الخطي ، سواء كُتب بخط اليد أو بالآلة الكاتبة ، وما يحتويه من البيانات ، وتوقيع أطرافه ، وتعدد النسخ في العقود المتبادلة ، والشكل الذي قد يفرضه القانون في حالات معينة.

هذا بالإضافة إلي معضلة تحديد القانون الواجب التطبيق علي العقود الرقمية الدولية وقوتها الثبوتية ، وإشكالية استعماله ، وإثباته، وطريقة تقديمه للمحكمة الناظرة في النزاع المتعلق به. وكذلك إشكالية تحديد مفهوم أصل السند الرقمي وصورته؛ إذ أن النسخة هي تكرار الأصل في كل جزئياته ، لذلك تعتبر النسخة أصلاً جديداً من دون تمييز بينهما.

لكن التساؤل الأساسي في هذا الصدد والذي يستتبع تبني الاستعانة بالوسائل الرقمية في التقاضي **هو**[2]:

---

[1] راجع في ذلك: د/عبد التواب مبارك ، الدليل الرقمي أمام القاضي المدني ، دار النهضة العربية ، بدون سنة نشر ، ص 8 وما بعدها.

[2] راجع في ذلك : د/ فاطمة عادل سعيد ، التقاضي عبر وسائل التكنولوجيا والاتصال الحديث ، الجزء الأول ، ص 395 وما بعدها .

- **كيف يمكن أن يضمن استخدام الوسائل الحديثة السرية[1] والرسمية في ذات الوقت للملفات التي يتم تبادلها رقميا سواء بين المحكمة والخصوم أو الخصوم بعضهم البعض؟**
- **هل هذه الآليات- أي الوسائل الرقمية- علي درجة من الكفاءة بحيث يمكن الاعتماد عليها في ضمان سلامة[2] البيانات المتداولة رقميا؟[3]**

---

[1] راجع في ذلك :

Mike L. Bridenback, Consultant ,Study of State Trial Courts Use of Remote Technology Final Report, National Association for Presiding Judges and Court Executive Officers, April 2016, p9-27

- http://www.law.georgetown.edu/library/collections/catalog/new-titles/august2012.cfm(تاريخ آخر دخول علي الموقع : 2021/1/8)

[2] راجع في ذلك : : ا .د / براء منذر كمال عبداللطيف ، ا .م .د / أمير حسن جاسم ، المستندات الرقمية وحجيتها في الإثبات ، مرجع سابق ، ص 4 وما بعدها ، وراجع أيضا :

- اتخاذ خيارات أفضل مع البيانات القانونية:
- https://www.lawtechnologytoday.org/2020/08/how-to-effectively-manage-data-breach-risks-from-third-parties/(تاريخ آخر دخول علي الموقع 2020/9/22)
- https://www.lawtechnologytoday.org/2020/08/make-better-choices-with-legal-data/(تاريخ آخر دخول علي الموقع 2020/9/22)
- https://www.lawtechnologytoday.org/2020/09/legal-teams-should-seek-forward-looking-ai-technology/(تاريخ آخر دخول علي الموقع 2020/9/22)

[3] يقصد بمصطلح **سلامة البيانات:** (التحقق من أن البيانات التي تضمنتها الوثيقة لم يحدث بها أي تعديل أو حذف سواء لأسباب طبيعية أو عمدية) ، راجع أيضا : د/ محمد محمد سادات ، حجية التوقيع الرقمي في الإثبات ، رسالة دكتوراه ، جامعة المنصورة ، ٢٠١٠ ، ص ١٩٥.

- **كيف يمكن التحكم في الصعوبات[1] المرتبطة باستخدام التكنولوجيا دون الإخلال بالتنظيم القضائي والضمانات الأساسية لحسن سير العدالة؟**

ذلك إن الإشكالية فيما يتعلق بالإثبات التي تثيرها الاستعانة بالوسائل الرقمية في التقاضي هي إنه في الوضع العادي عندما يوجد ملف ورقي وآخر رقمي، فيمكن الوقوف علي صحة الأخير بمقارنته بالأول، أما في فرض البيئة الرقمية والدليل الرقمي كيف يمكن التحقق من سلامة بيانات مستند معين (ويمكن التعويل عليه في الإجراءات عموما خاصة أن التبديل أو التعديل في الملفات الرقمية لا يترك أي أثر عليه و العكس) من هذا النقد يري البعض أن أي عيوب تتبدي في النظام الرقمي لا يمكن أن تتساوي بحال من الأحوال مع الوضع قبل الاستعانة بتكنولوجيا المعلومات في القضاء.

إن الذي يضفي الرسمية علي الأوراق المستندات في النظام الورقي هو التوقيع ،[2]وهو نفس الآلية التي سوف يعتمدها المشرع لإضفاء الرسمية علي المحررات الرقمية. وبناءا علي ما سبق يجب الوقوف علي أهم مصطلحات الإثبات الرقمي : كالدليل الرقمي ، التوقيع الرقمي ،

---

[1] راجع في ذلك : راجع في ذلك : د/ فاطمة عادل سعيد ، التقاضي عبر وسائل التكنولوجيا والاتصال الحديث ، مرجع سابق ، الجزء الأول ، ص 379 وما بعدها ، وراجع أيضا :

- http://www.worldcat.org/title/electronic-technology-and-civil-procedure-new-paths-to-justice-from-around-the-world/oclc/773670695 (تاريخ آخر دخول علي الموقع : 2021/1/8)
- https://www.sal.org.sg/Resources-Tools/Legal-Technology-Vision
- https://digitalcommons.osgoode.yorku.ca/cgi/viewcontent.cgi?article=2378&context=scholarly_works
- https://www.tandfonline.com/doi/full/10.1080/17579961.2020.1815404 (تاريخ آخر دخول علي الموقع 2020/9/22)
- https://v1.lawgazette.com.sg/2001-11/Nov01-focus2.htm(تاريخ آخر دخول علي الموقع 22/9/2020)

[2] راجع في ذلك : د/أحمد محمود أحمد ، أحكام المستند الرقمي ، مرجع سابق ، ص 120 وما بعدها.

المحررات الرقمية ، و التعرض بالضرورة لبعض الجوانب الفنية بالقدر اللازم كأليات التوثيق، التشفير ، و الوقوف علي أهم إشكاليات قبول الأدلة بالإثبات الرقمي[1].

المطلب الأول

ماهية الأدلة الرقمية[2]

الأدلة الرقمية[3] ، والتي تُعرف أحيانًا **بالأدلة الرقمية**[4] ، أو **بالأدلة السيبرانية هي**[5] مصطلح يشير إلي المعلومات الإثباتية التي يتم إرسالها أو تخزينها بتنسيق رقمي والتي يمكن

---

[1] راجع في ذلك :

- Koulika Arnaud NIKIEMA، La preuve dans le contentieux du cyberespace ،Université Gaston Berger de Saint Louis du Senegal – Master pro (DESS)Droit du cyberespace 2011،p6

[2] راجع في ذلك :

- Mike L. Bridenback, Consultant ,Study of State Trial Courts Use of Remote Technology Final Report, National Association for Presiding Judges and Court Executive Officers, April 2016, p2-27

http://www.abanet.org/litigation/discoverystandards/2004civildiscoverystandards.pdf

3راجع فى ذلك : د/أمل فوزى أحمد،بحث بعنوان " الأدلة الرقمية في الإثبات بين معايير القبول وأمن المعلومات "، منشور بالمجلة الدولية للاجتهاد القضائي : العدد الثاني يوليو – تموز 2021 ،المجلد 1 – المركز_الديمقراطي_العربي المانيا– برلين

[4] راجع في ذلك : د. محمد كمال شاهين ، حجية الدليل الرقمي في الإثبات الجنائي . دراسة مقارنة ، المؤتمر العلمي الخامس (الافتراضي) ، كلية الحقوق جامعة السلطان قابوس ، " نظم التقاضي وتحديث قواعد الإثبات "تطوير نظم التقاضي وتحديث قواعد الإثبات" ، ٢٢ ديسمبر ٢٠٢٠ ، ص 4 وما بعدها ، و راجع أيضا : تاريخ آخر دخول : (تاريخ آخر دخول: 2021/1/20)

- https://phys.org/news/2015-03-digital-forensics.html
- https://www.lawgazette.co.uk/news/law-enforcers-struggle-with-electronic-evidence-challenges-/5066471.article

[5] راجع في ذالك : (تاريخ آخر دخول: 2020/11/12)

- http://www.stephenmason.eu/articles/electronic-evidence.html

استخدامها بعد ذلك في محاكمة أو دعوي قضائية. قبل قبول الأدلة الرقمية[1] من قبل المحكمة ، يجب تحديد ما إذا كان هذا الدليل أصيلًا أو ذا صلة أو إشاعات أو ما إذا كان سيتم قبول النسخ أو ما إذا كان يجب تقديم الأصل[2] .

عرف المشرع **الدليل الرقمي**[3] بإنه : (أية معلومات رقمية لها قوة أو قيمة ثبوتية مخزنة أو منقولة أو مستخرجة أو مأخوذة من أجهزة الحاسب أو الشبكات المعلوماتية وما في حكمها ، والممكن تجميعها وتحليلها باستخدام أجهزة أو برامج أو تطبيقات تكنولوجية خاصة) .(م1 قانون 175 لسنة 2018)

ومن التعريف السابق يتضح أن الدليل الرقمي ما هو إلا عبارة عن معلومات رقمية[4] والمعلومات الرقمية هي كل ما يمكن إنشاؤه أو تخزينه ، أو معالجته ، أو تخليقه ، أو نقله ، أو مشاركته ، أو نسخه بواسطة تقنية المعلومات ؛ كالأرقام والأكواد والشفرات والحروف والرموز والإشارات والصور والأصوات وما في حكمها ، و لها قوة أو قيمة ثبوتية. مخزنة أو منقولة أو مستخرجة أو مأخوذة من أجهزة الحاسب أو الشبكات المعلوماتية وما في حكمها علي دعامة رقمية (أي وسيط مادي لحفظ وتداول البيانات والمعلومات الرقمية ومنها الأقراص المدمجة أو

---

[1] راجع في ذالك (تاريخ آخر دخول: 2021/1/3)

حول القبول القانوني للأدلة الرقمية:

_ https://www.tandfonline.com/doi/abs/10.1080/13600860420002235 08?src=recsys&journalCode=cirl20

[2] راجع في ذالك : (تاريخ آخر دخول: 2021/1/12)

حول مقبولية الأدلة الرقمية في المحكمةAEEC)): نتائج دراسة أوروبية : (تاريخ آخر دخول: 2021/1/12)

_ https://www.tandfonline.com/doi/full/10.1080/15567280701418049?src=recsys

[3] راجع في ذالك : (تاريخ آخر دخول: 2021/1/12)

_ http://www.stephenmason.eu/articles/electronic-evidence.html

[4] راجع في ذلك : د/ عبد العزيز سعد بن دخيل الغانم ، المحكمة الرقمية ، دراسة تأصيلية ، رسالة دكتوراه ، مرجع سابق ، ص113 وما بعدها .

الأقراص الضوئية أو الذاكرة الرقمية أو ما في حكمها) ، والممكن تجميعها وتحليلها باستخدام أجهزة أو برامج أو تطبيقات تكنولوجية خاصة. (م1 قانون 175 لسنة 2018)

ولقد اعترف المشرع بالمادة (11) من قانون 175 لسنة 2018 **بحجية الأدلة الرقمية**[1] فنص علي[2] :

(يكون للأدلة المستمدة أو المستخرجة من الأجهزة أو المعدات أو الوسائط الدعامات الرقمية، أو النظام المعلوماتي أو من برامج الحاسب ، أو من أي وسيلة لتقنية المعلومات نفس قيمة وحجية الأدلة الجنائية المادية في الإثبات الجنائي[3] متي توافرت بها الشروط الفنية الواردة باللائحة التنفيذية) .

وبناءا علي سبق نستنتج اعتراف المشرع بالدليل الرقمي وحجيته[4] وهو ما يؤيده حكم محكمة القاهرة الاقتصادية في الجنحة رقم 225 لسنة 2018 جنح مستأنف ورقم 1807 لسنة 2017 جنح اقتصادي بقبولها لأدلة رقمية بالدعوي كرسائل الهاتف المحمول وحساب موجود علي موقع التواصل الاجتماعي face book ورسائل موجودة علي ال whats app.[5]

---

[1] هل يمكن استخدام المستندات الرقمية كدليل ؟ راجع : (تاريخ آخر دخول: 2021/1/12)

_ https://www.lawteacher.net/free-law-essays/international-law/can-electronic-documents-be-used-as-evidence-international-law-essay.php

[2] راجع في ذلك: د/عبد التواب مبارك ، الدليل الرقمي أمام القاضي المدني ، مرجع سابق ، ص 13 وما بعدها.

[3] حول مقبولية الأدلة الرقمية ، راجع : (تاريخ آخر دخول: 2021/1/12)

_ https://www.crime-scene-investigator.net/admissibilitydigitaleveidencecriminalprosecutions.html

[4] راجع في ذلك: د/عبد التواب مبارك ، الدليل الرقمي أمام القاضي المدني ، مرجع سابق ، ص 50 وما بعدها.

[5] راجع في ذلك : د./ محمد كمال شاهين ، حجية الدليل الرقمي في الإثبات الجنائي . دراسة مقارنة ، مرجع سابق، ص11 وما بعدها ، و راجع أيضا : (تاريخ آخر دخول: 2021/1/12)

_ http://www.stephenmason.eu/articles/electronic-evidence.html

ومن الغريب أن المشرع[1] قد قصر الاعتراف بالدليل الرقمي علي القاضي الجنائي دون القاضي المدني علي الرغم من مساواته في الأهمية علي المستويين (القضاء المدني والقضاء الجنائي) ، لهذا تري الباحثة ضرورة اعتراف[2] المشرع بالدليل الرقمي في القانون المدني تيسيرا علي المتقاضين بالدعوي الرقمية ، وإجراءات التقاضي الرقمي وإدخال تعديل علي نص المادة 11 من قانون رقم 175 لسنة2018 ليشمل اعتراف المشرع بالدليل الرقمي أمام القاضي المدني كما اعترف بحجيته أمام القاضي الجنائي [3] .

---

[1] كما عاقب المشرع بالمادة 17من قانون 175 لسنة 2018علي **جريمة الإعتداء علي سلامة البيانات والمعلومات والنظم المعلوماتية: حيث نص علي:** (يعاقب بالحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن100 ألف جنيه ولا تجاوز 500 ألف جنيه، أو بإحدى هاتين العقوبتين كل من أتلف أو عطل أو عدل مسار أو ألغي كلياً أو جزئياً، متعمداً وبدون وجه حق، البرامج والبيانات أو المعلومات المخزنة، أو المعالجة، أو المولدة أو المخلقة علي أي نظام معلوماتي وما في حكمه، أيا كانت الوسيلة التي استخدمت في الجريمة) .

[2] حول المقبولية القانونية للأدلة الرقمية، راجع : (تاريخ آخر دخول: 2021/1/12)

_ https://www.tandfonline.com/doi/abs/10.1080/13600860420002235 08?src=recsys&journalCode=cirl20

[3] راجع في ذالك : د. محمد كمال شاهين ، حجية الدليل الرقمي في الإثبات الجنائي ، مرجع سابق ، ص11 وما بعدها ، وراجع أيضا : (تاريخ آخر دخول: 2021/1/12)

_ https://www.crime-scene-investigator.net/admissibilitydigitaleveidencecriminalprosecutions.html

_ https://blog.signaturit.com/en/electronic-evidence-and-its-admissibility-in-court

_ https://www.tamimi.com/law-update-articles/admissibility-and-reliability-of-electronic-evidence-before-qatari-courts/

_ https://www.bcs.org/content-hub/presenting-digital-evidence-to-court/

_ https://www.atlanticdf.com/blog/2017/12/18/admissibility-of-digital-evidence-in-court/

_ https://www.ukessays.com/essays/criminology/presenting-digital-evidence-to-court-criminology-essay.php

ولقد ازداد استخدام الأدلة الرقمية[1] في العقود القليلة الماضية، حيث سمحت المحاكم باستخدام رسائل البريد الرقمي ، الصور الرقمية ، أجهزة الصراف الآلي سجلات المعاملات، معالجة النصوص وثائق، والملفات المحفوظة من المحاسبة برامج، جداول البيانات ، متصفح الإنترنت وتاريخها، قواعد البيانات ، ومحتويات ذاكرة الكمبيوتر ، والنسخ الاحتياطية للكمبيوتر ، والمطبوعات الخاصة بالكمبيوتر ، ومسارات نظام تحديد المواقع العالمي GPS ، والسجلات من أقفال أبواب الفنادق الرقمية ، والفيديو الرقمي أو الملفات الصوتية[2] .

- **إيجابيات وسلبيات الأدلة الرقمية[3] :**

فيما يتعلق بموثوقية هذه الأدلة ، يعتقد بعض القضاة أن دقة وموضوعية الأدلة الرقمية تجعلها أكثر موثوقية في حين يعتقد قضاة آخرون أن الافتقار إلي الوسائل اللازمة للتحقق من صحة الأدلة الرقمية[4] يجعلها أكثر عرضة للخطر وبالتالي ، فهي أقل موثوقية من الأدلة

---

[1] راجع في ذلك : (تاريخ آخر دخول: 2021/1/12)

_ https://en.wikipedia.org/wiki/Digital_evidence Tech. 5 (2011

[2] راجع في ذلك : (تاريخ آخر دخول: 2021/1/12)

_ https://www.crime-scene-investigator.net/admissibilitydigitaleveidencecriminalprosecutions.html

_ https://blog.signaturit.com/en/electronic-evidence-and-its-admissibility-in-court

_ https://www.tamimi.com/law-update-articles/admissibility-and-reliability-of-electronic-evidence-before-qatari-courts/

_ https://www.bcs.org/content-hub/presenting-digital-evidence-to-court/

_ https://www.atlanticdf.com/blog/2017/12/18/admissibility-of-digital-evidence-in-court/

_ https://www.ukessays.com/essays/criminology/presenting-digital-evidence-to-court-criminology-essay.php

[3] راجع في ذلك : (تاريخ آخر دخول: 2021/1/12)

_ https://www.tandfonline.com/doi/full/10.1080/15567280701418049?src=recsys

[4] حول تفاصيل اكثر عن الأدلة الرقمية، راجع : (تاريخ آخر دخول: 12/1/2021)

_ https://en.wikipedia.org/wiki/Digital_evidence

التقليدية عمومًا.

هذا ويبرز العديد من الخبراء التقنيين **بعض الخصائص الإيجابية حول الأدلة الرقمية** فهي : دقيقة ، كاملة ، واضحة ، دقيقة ، حقيقية ، موضوعية ، ومحايدة. في كثير من الحالات ، يبدو أن الأدلة الرقمية ضرورية لحل نوع معين من الجرائم. بالنسبة للقضاة ، من السهل جمع الأدلة الرقمية وتخزينها وحفظها. بشكل عام . وبالنظر الي النظم القضائية المقارنة نجد بالمملكة المتحدة ، قانون للشرطة والأدلة الجنائية ، والذي ينظم جمع "أدلة الكمبيوتر" بطريقة محددة [1]. كما تضمن القانون البلجيكي لجرائم الكمبيوتر بعض التعاليم حول جمع الأدلة التي يمكن تطبيقها أيضًا علي الأدلة الرقمية.

و**فيما يتعلق بسلبيات الأدلة الرقمية**[2] ، يري أخصائيو القانون أن تحديد القيمة القانونية لهذا النوع من الأدلة يمثل صعوبة بسبب الجهل الحالي بإجراءات معالجة البيانات[3]. وتنشأ هذه الصعوبة بسبب عدم وجود تنظيم مناسب ومنتظم وكذلك عدم وجود فقه متجانس. وبالنسبة لخبراء الكمبيوتر ، تتمثل بعض السلبيات في الافتقار إلي الدعم القانوني ونماذج الشهادات ،

---

[1] راجع في ذلك : (تاريخ آخر دخول: 2021/1/12)

_ https://www.unodc.org/e4j/en/cybercrime/module-6/key-issues/handling-of-digital-evidence.html

[2] حول مشاكل الاستخدام في الوثائق الرقمية كدليل في العملية المدنية ،راجع : (تاريخ آخر دخول: 12/1/2021)

_ http://aurora.turiba.lv/editor/Conference14/vBook/proceeding/pages/EN030_Simeblyte_Nemeiksis/EN030_Simeblyte_Nemeiksis.htm

[3] راجع في ذلك : (تاريخ آخر دخول: 12/1/2021)

_ https://docplayer.net/10509033-Content-management-for-courts-improve-court-operations-by-reducing-costs-speeding-response-times-and-simplifying-paper-intensive-processes.html

ونقص الفهم الذي أبدته الهيئات القضائية في أوروبا[1] ، فضلاً عن التكاليف الباهظة المتعلقة بالحصول علي الأدلة الرقمية وتفسيرها[2] ، وهي مهمة تستغرق وقتًا كبيرًا. كما لا تشمل المعايير الإجرائية أي إجراء محدد لتنظيم جمع الأدلة الرقمية وحفظها وعرضها في المحكمة. وفقًا لجميع الموثقين الذين تمت مقابلتهم ، لا يوجد أي إجراء محدد لحفظ الأدلة الرقمية ، والإجراءات الوحيدة التي ذكروها هي تلك الخاصة بإنشاء التوقيعات الرقمية.

- **دور الأدلة الرقمية:**

يمكن أن تكون الأدلة الرقمية مفيدة في مجموعة واسعة من التحقيقات المدنية والجنائية فعلي سبيل المثال في تفجيرات مركز التجارة العالمي في الولايات المتحدة في عام 2001 ، لعبت أجهزة الكمبيوتر دورًا في التخطيط والتحقيقات اللاحقة لكل من الهجومين حيث تم اكتشاف أن المشتبه بهم وأجهزة الكمبيوتر المحمولة الخاصة كانت تحتوي علي خطط للتفجير الأول وخلال التحقيق في الهجوم الثاني ، تم فحص أكثر من 100 محرك أقراص صلبة[3].

وفي عام 1996 ، تم إجراء تحقيق رقمي آخر في قضية شارون لوباتكا ، من ولاية ماريلاند في الولايات المتحدة. قامت بالتحقيقات الشرطة حيث عثرت علي المئات من رسائل البريد الرقمي بين لوباتكا ورجل يدعي روبرت غلاس بشأن تعذيبهم وأوهامهم. وهو ما قاد المحققين إلي ولاية كارولينا الشمالية حيث تم العثور علي قبر Lopatka .

---

[1] حول مقبولية الأدلة الرقمية في المحكمة : (تاريخ آخر دخول: 2021/1/12)
https://www.tandfonline.com/doi/full/10.1080/15567280701418049?src=recsys

[2] راجع في ذلك : (تاريخ آخر دخول: 2021/1/12)
- https://www.lawgazette.co.uk/news/law-enforcers-struggle-with-electronic-evidence-challenges-/5066471.article

[3] راجع في ذلك:
Sophia BINET، L'utilisation des nouvelles technologies dans le procès civil : Vers une procédure civile intégralement informatisée، p65.

- **تصنيف الأدلة الرقمية[1] :**

قد يشتمل المستند الرقمي إما علي مستندات مخزنة في شكل رقمي أو مطبوع عليها. إن ما يتم تسجيله رقميًا هو مستند بالمعني الدقيق للكلمة ، ولكن لا يمكن أن يتصوره شخص لا يستخدم نظام الكمبيوتر الذي تم فيه تغذية هذه المعلومات في البداية. هكذا ، إذا كان الملحن الموسيقيA يمزج بعض الألحان علي جهاز الكمبيوتر الخاص به ، ويريد ملحن آخر ، B ، مقاضاته بسبب انتهاك حقوق النشر ، فلن يتمكن B من الوصول إلي السجلات الرقمية علي جهاز الكمبيوتر الخاص بـ A. علي الرغم من إمكانية طباعة مثل هذا المستند علي قاعدة مغناطيسية ، مثل قرص مضغوط (CD) ، إلا أنه لا يزال يتطلب الوصول إلي جهاز الكمبيوتر الخاص بـ A. يمكن لأي شخص أن ينظر إلي المستند الذي يحتوي علي نسخة مطبوعة من سجلات الكمبيوتر ، علي الرغم من وجود مستند مثل هذه المطبوعات من الوثائق ستكون بمثابة دليل ثانوي يخضع لأحكام قانون الأدلة الهندي. فبموجب قانون الأدلة الهندي ، يمكن اعتبار أي مادة تم التعبير عنها أو وصفها بشأنها وثيقة ، شريطة أن يكون الغرض من هذا التعبير أو الوصف هو تسجيل الأمر، و تم تعريف السجلات الرقمية في قانون تكنولوجيا المعلومات لعام 2000 علي أنها أي بيانات أو سجل أو بيانات تم إنشاؤها أو أي صورة أو صوت مخزّن أو مستلم أو مرسَل في شكل رقمي أو فيلم مصغر أو غشاء مصغر تم إنشاؤه بواسطة الكمبيوتر. يمكن تضمين السجل الرقمي بأمان في ظل هذا التعريف لأن المادة تُسجَّل علي الكمبيوتر باعتبارها وحدات البت والبايت ، وهي المكافئ الرقمي للأرقام أو العلامات .

ونظرًا لوجود أدلة سمعية وثانوية[2] ، كان هناك الكثير من التردد فيما يتعلق بقبول السجلات الرقمية كدليل[3]. ولكن اعتُبرت سجلات الكمبيوتر علي نطاق واسع بمثابة بيانات

---

[1] راجع في ذالك : (تاريخ آخر دخول: 2021/1/12)

_ https://www.lawteacher.net/free-law-essays/commercial-law/relevancy-and-admissibility-of-electronic-law-essays.php

[2] راجع في ذلك : د/ عبد العزيز سعد بن دخيل الغانم ، المحكمة الرقمية ، دراسة تأصيلية ، رسالة دكتوراه ، مرجع سابق ، ص118 وما بعدها ، ص 138 وما بعدها .

[3] راجع في ذلك : (تاريخ آخر دخول: 2021/1/12)

سماعية لأن أي معلومات يتم استرجاعها من جهاز كمبيوتر ستتألف من مدخلات يقدمها إنسان. وبالتالي ، سواء كانت وثيقة كاملة تحتوي علي عبارات مكتوبة من قبل طرف واحد ، أو صورة لشخص مفقود تم إنشاؤها بواسطة الكمبيوتر بناءً علي المدخلات المقدمة إليه ، فستكون كل هذه السجلات قابلة للسمع. و تم قبول المستندات الرقمية بالمعني الدقيق للكلمة كدليل حقيقي ، أي أدلة مادية ، ولكن هذا الدليل يتطلب شهادة فيما يتعلق بموثوقية الجهاز في القبول

_ https://www.tandfonline.com/doi/abs/10.1080/13600860420002235 08?src=recsys&journalCode=cirl20

_ https://www.tandfonline.com/doi/full/10.1080/15567280701418049?src=recsys

_ https://www.crime-scene-investigator.net/admissibilitydigitaleveidencecriminalprosecutions.html

_ https://blog.signaturit.com/en/electronic-evidence-and-its-admissibility-in-court

المطلب الثاني

متطلبات الإثبات بالأدلة الرقمية[1]

- **الإثبات بالأدلة الرقمية[2] في القضايا المدنية[3] :**

القواعد التي تحكم الإثبات في القضايا المدنية وكيف يمكن أن تؤثر علي عملية الإثبات من الممكن أن تكون تحديا لعدة أسباب للقضاء المدني. فبالنسبة للمدعي ، فسوف يواجه محاولة معرفة ما هي الأدلة التي قد تكون موجودة في قضيته ، وأين توجد ومكانها وزمانها ففرصة ضياع الأدلة أو إتلافها في قضية مدنية هي في الواقع أعلي بكثير مما هي عليه في قضية جنائية. والسبب في ذلك هو أن الشخص أو الأشخاص المعنيين قد يعلمون مقدمًا جيدًا أنك ستسعي للحصول علي الأدلة الرقمية وقد يتخذون خطوات للتخلص من أي شيء يدينهم بأسرع ما يكون ودون أثر ، بينما في حالة القضايا الجنائية ، عادة ما يتم ضبط الأدلة دون إنذار مسبق من الأشخاص الذين بحوزتهم الدليل[4].

- **المبادئ التي تؤثر علي قبول الأدلة الرقمية[5] :**

---

[1] راجع في ذلك: د/عبد التواب مبارك ، الدليل الرقمي أمام القاضي المدني ، مرجع سابق ، ص 13 وما بعدها.

[2] راجع في ذلك: د/عبد التواب مبارك ، الدليل الرقمي أمام القاضي المدني ، مرجع سابق ، ص 58 وما بعدها.

[3] راجع في ذلك :

_ https://www.tamimi.com/law-update-articles/admissibility-and-reliability-of-electronic-evidence-before-qatari-courts/

_ https://www.bcs.org/content-hub/presenting-digital-evidence-to-court/

_ https://www.atlanticdf.com/blog/2017/12/18/admissibility-of-digital-evidence-in-court/

[4] راجع في ذلك :

_ https://www.sciencedirect.com/science/article/pii/B978159749643800016X

[5] للتفصيل أكثر راجع في ذلك كلا من : (تاريخ آخر دخول: 2021/1/12)

_ حول المقبولية القانونية للأدلة الرقمية، راجع:

تلعب المبادئ المتعلقة بالفعالية والفائدة والشرعية دورًا مهمًا في التشريعات الأوروبية المختلفة في مجال قبول الأدلة الرقمية . إن الحاجة إلي الحصول علي أدلة ، والشفافية أثناء جمعها ، واحترام حرية التعبير هي مبادئ تنعكس في المعايير في أوروبا ، ولكن لها وضع ثانوي فيما يتعلق بقبول الأدلة.

- https://www.tandfonline.com/doi/abs/10.1080/13600860420002235 08?src=recsys&journalCode=cirl20

_ حول صعود الطب الشرعي الرقمي، راجع:

- https://www.lexology.com/library/detail.aspx?g=29828d6d-8396-4070-9424-05ac2e0ecfae

_ حول الأدلة الرقمية ومقبوليتها في المحكمة ، راجع:

- https://blog.signaturit.com/en/electronic-evidence-and-its-admissibility-in-court

_ حول مقبولية الأدلة الرقمية في الدعاوي الجنائية، راجع:

- https://www.crime-scene-investigator.net/admissibilitydigitaleveidencecriminalprosecutions.html

_ حول قبول الأدلة الرقمية ، راجع:

- https://www.mailxaminer.com/blog/admissibility-of-electronic-evidence-in-court/

_ حول أهمية ومقبولية الأدلة الرقمية ، راجع:

_ https://www.lawteacher.net/free-law-essays/commercial-law/relevancy-and-admissibility-of-electronic-law-essays.php

_ حول قبول وموثوقية الأدلة الرقمية أمام المحاكم القطرية ، راجع:

- https://www.tamimi.com/law-update-articles/admissibility-and-reliability-of-electronic-evidence-before-qatari-courts/

_ حول قبول الأدلة الرقمية ، راجع:

_ https://articles.forensicfocus.com/2017/06/29/an-introduction-to-challenges-in-digital-forensics/

_ https://www.unodc.org/e4j/en/cybercrime/module-6/key-issues/handling-of-digital-evidence.html

فالمبادئ التي تؤثر علي الأدلة الرقمية هي أساسًا: **احترام معايير حماية البيانات** ; **واحترام سرية الاتصالات; وحق حرية التعبير**[1].

وفي الممارسة العملية ، يذكر الفقهاء الأوروبيون إن مبادئ الشرعية ، وملاءمة الصلة ، واستخدام هذه الأدلة لها تأثير أكبر. كما يؤكد الخبراء الفنيون علي أنهم يتصرفون وفقًا لاحترام الحقوق الفردية. علي سبيل المثال ، يذكر خبراء الطب الشرعي الرقمي[2] من ألمانيا واليونان احترام معايير حماية البيانات ، بينما يسلطون الضوء في فرنسا ولوكسمبورغ وأيرلندا علي الحفاظ علي السرية. بينما يفضل المتخصصون في إيطاليا والمملكة المتحدة تطوير وظائفهم من خلال المواد المشفرة كمبادئ أساسية. علاوة علي ذلك ، يذكر خبراء آخرون إن بإمكانهم الاعتماد علي الدعم القانوني القادم من كاتب عدل أو شاهد ، كما في إسبانيا ورومانيا.

---

[1] راجع في ذلك : (تاريخ آخر دخول: 2021/1/12)

_ https://articles.forensicfocus.com/2017/06/29/an-introduction-to-challenges-in-digital-forensics

_ https://www.unodc.org/e4j/en/cybercrime/module-6/key-issues/handling-of-digital-evidence.html

2 راجع في ذلك كلا من : (تاريخ آخر دخول: 2021/1/12)

حول تحديات الطب الشرعي الرقمي ، راجع:

_ https://phys.org/news/2015-03-digital-forensics.html

حول الطب الشرعي الرقمي ، راجع :

_ https://www.researchgate.net/publication/327644306_Digital_Forensics_Review_of_Issues_in_Scientific_Validation_of_Digital_Evidence

_ https://economictimes.indiatimes.com/news/politics-and-nation/courts-can-rely-on-electronic-records-without-certificate-supreme-court/articleshow/62777759.cms

_ http://www.jurisdiction.com/ecom4.htm

_ https://www.lexology.com/library/detail.aspx?g=29828d6d-8396-4070-9424-05ac2e0ecfae

- **خطوات جمع واستخدام الأدلة الرقمية[1] :**

هناك عدد من الخطوات التي يجب الأخذ بها في الاعتبار عند جمع واستخدام الأدلة الرقمية هي:

- الحصول علي الأدلة الرقمية .
- دمج الأدلة الرقمية .
- الامتثال للمتطلبات الإجرائية .
- تقييم الأدلة الرقمية.

- **تقديم وتقييم[2] الأدلة الرقمية بالمحكمة[3] :**

عند إجراء التقييم للأدلة الرقمية[4] ، ينبغي علي القاضي أن يضع في اعتباره موقف كل طرف فيما يتعلق بحجية الأدلة الرقمية[5] المقدمة ، خاصة إذا رفض الطرف المعارض

---

[1] راجع في ذلك : (تاريخ آخر دخول: 2021/1/12)

_ https://ci.security/resources/news/article/3-methods-to-preserve-digital-vidence-for-computer-forensics

[2] راجع في ذلك : د/ الأنصاري حسن النيداني، القاضي والوسائل الرقمية الحديثة ، مرجع سابق، ص99 وما بعدها .

[3] راجع في ذلك كلا من : (تاريخ آخر دخول: 2021/1/12)

_ عن كيفية تقديم الأدلة الرقمية في المحكمة ؟ ، راجع:

_ https://www.atlanticdf.com/blog/2017/12/18/admissibility-of-digital-evidence-in-court/

_ حول تقديم الأدلة الرقمية للمحكمة ، راجع:

_ https://www.ukessays.com/essays/criminology/presenting-digital-evidence-to-court-criminology-essay.php

[4] راجع في ذلك : (تاريخ آخر دخول: 2021/1/12)

_ https://blog.signaturit.com/en/electronic-evidence-and-its-admissibility-in-court

[5] راجع في ذلك : د/أحمد محمود أحمد ، أحكام المستند الرقمي ، مرجع سابق ، ص 171 وما بعدها.

(اعتراض) صلاحية الدليل وطعن فيه . فإذا كان هناك اعتراض ، فإن الحجج التي تدعم رفضها وتلك التي تُظهر الأدلة وآراء الخبراء لإثبات صحتها تكون ذات صلة بالقاضي وشانه في تكوين عقيدته .

أما إذا لم يتم تقديم أي اعتراض ، مما يعني أنه لم يتم التشكيك[1] في صحة الأدلة الرقمية ، فيتعين علي القاضي اعتبارها أصلية ودقيقة ، وسيقيمها جنبًا إلي جنب مع بقية الأدلة.

وبالتالي ، في الممارسة العملية ، يجب علي الطرف الذي يسعي إلي صحة الأدلة الرقمية تقديم جميع الأدلة الممكنة لتعزيز الأدلة المقدمة ، و هي عادة تعزز مع خبير بالأدلة الرقمية يثبت صحة البيانات وعدم التلاعب بها[2].

---

[1] راجع في ذلك : (تاريخ آخر دخول: 2021/1/12)

- https://ci.security/resources/news/article/3-methods-to-preserve-digital-evidence-for-computer-forensics
- https://phys.org/news/2015-03-digital-forensics.html
- https://www.lawgazette.co.uk/news/law-enforcers-struggle-with-electronic-evidence-challenges-/5066471.article

[2] راجع في ذلك : (تاريخ آخر دخول: 2021/1/12)

- https://www.tandfonline.com/doi/abs/10.1080/13600860420002235 08?src=recsys&journalCode=cirl20
- https://www.tandfonline.com/doi/full/10.1080/15567280701418049?src=recsys
- https://www.crime-scene-investigator.net/admissibilitydigitaleveidencecriminalprosecutions.html
- https://blog.signaturit.com/en/electronic-evidence-and-its-admissibility-in-court

وعلي الرغم من أن الطريقة الرئيسية لتوفير الأدلة الرقمية هي طباعة المعلومات علي الورق وتقديم البيانات الرقمية في وسيط مثل قرص مضغوط ، حتي يتوفر الدليل المذكور للحصول علي أمان حقيقي ، يجب أن يرجع فيه إلي خبير بالأدلة الرقمية[1].

باختصار ، إن الأمر يتعلق بإحضار جميع أنواع الأدلة التي المتاحة لإقناع القاضي بصحة الأدلة الرقمية المقدمة ، والحماية من التحدي الافتراضي (الطعن علي الدليل2) للطرف المعارض.

[1] راجع في ذلك : (تاريخ آخر دخول: 2021/1/12)

- https://www.ukessays.com/essays/criminology/presenting-digital-evidence-to-court-criminology-essay.php
- https://articles.forensicfocus.com/2017/06/29/an-introduction-to-challenges-in-digital-forensics
- https://www.unodc.org/e4j/en/cybercrime/module-6/key-issues/handling-of-digital-evidence.html

[2] راجع في ذلك: د/عبد التواب مبارك ، الدليل الرقمي أمام القاضي المدني ، مرجع سابق ، ص 110 وما بعدها.

المطلب الثالث

أنواع[1] الأدلة الرقمية[2]

أولا : المحرر الرقمي[3] ،الكتابة الرقمية:

يعرف **المحرر الرقمي** [4] بإنه:" المعلومات والبيانات المسجلة رقميا[5] والتي تم تبادلها رقميا باستخدام نظام معالجة المعلومات عبر وسيط رقمي[6]. " الأمر الذي يمكن القول معه أن المراسلات بين المحكمة والخصوم بحسب التعبير هي محررات رقمية كما في نظام رفع الدعوي E-Filing رقميا .

---

1 راجع في ذلك :

_ https://www.lawteacher.net/free-law-essays/international-law/can-electronic-documents-be-used-as-evidence-international-law-essay.php

[2] **المادة (11) من قانون 175 لسنة 2018في الأدلة الرقمية :**

(يكون للأدلة المستمدة أو المستخرجة من الأجهزة أو المعدات أو الوسائط الدعامات الإليكترونية، أو النظام المعلوماتي أو من برامج الحاسب، أو من أي وسيلة لتقنية المعلومات نفس قيمة وحجية الأدلة الجنائية المادية في الإثبات الجنائي متي توافرت بها الشروط الفنية الواردة باللائحة التنفيذية) .

[3] راجع في ذلك : محمد جميل إبراهيم ، اثر التقنيات الحديثة في مجال الدليل الكتابي ، رسالة دكتوراه ، كلية الحقوق ، جامعة الزقازيق، ص135 وما بعدها .

4 راجع في ذلك : عقد البيع عبر الإنترنت ، د. عمر خالد محمد الزريقات ، دراسة تحليلية ، رسالة دكتوراه، ج. عين شمس ، ص ١٩١ .

5 **ولقد عرفت المادة الأولي من قانون 175 لسنة 2018 البيانات الرقمية بانها :**

(البيانات والمعلومات الإليكترونية: كل ما يمكن إنشاؤه أو تخزينه ، أو معالجته ، أو تخليقه ، أو نقله ، أو مشاركته ، أو نسخه بواسطة تقنية المعلومات ؛ كالأرقام والأكواد والشفرات والحروف والرموز والإشارات والصور والأصوات وما في حكمها) .

6 هذا وقد نصت المادة 13 من قانون 146 لسنة 2019 بتعديل بعض أحكام قانون المحاكم الاقتصادية الصادر بالقانون رقم 120 لسنة 2008 علي تحديد المقصود بالمستند أو المحرر الرقمي انه:

(رسالة بيانات تتضمن معلومات تنشا أو تدمج أو تخزن أو ترسل أو تستقبل كليا أو جزئيا بوسيلة رقمية أو رقمية أو ضوئية أو بغيرها من الوسائل المشابهة. وهو ما يمكن القياس عليه والاستئناس به في مجال إجراءات التقاضي الرقمي أمام القضاء المدني) .

وبناءا علي ما سبق تُعد المحررات الرقمية[1] من قبيل المحررات المعترف بها ولها ذات الحجية المقررة للمحررات الرسمية أو العرفية في أحكام قانون الإثبات في المواد المدنية والتجارية وفي نطاق المعاملات المدنية والتجارية والإدارية .

1. المحررات الرسمية الرقمية[2]:

بحسب تعريف المحرر الرسمي وفقا للمادة العاشرة من قانون الإثبات المصري باعتباره المحرر الذي يثبت فيه موظف عام أو شخص مكلف بخدمة عامة ما تم علي يديه أو ما تلقاه من ذوي الشأن، فإن المحرر الرقمي لن يختلف في تعريفه عن المحرر الورقي إلا مع مراعاة خصوصية التكنولوجيا فيكون هذه العملية يوثق المرسل البصمة الرقمية باستخدام المفتاح الخاص الذي هو بمثابة توقيع بشكل رقمي، ثم يقوم بعملية الإرسال وعند وصول الرسالة إلي المرسل إليه يتأكد من صحة التوقيع الرقمي بإرسال نسخة منه إلي الجهة التي أصدرته أو من خلال الشهادة الرقمية التي بعثها المرسل إلي المرسل إليه مع المحرر الرقمي وهو ما يطلق عليه التصديق الرقمي وفي حالة التأكد من صحة التوقيع الرقمي يقوم المرسل إليه بخطوة أخيرة، وهي إعادة حساب البصمة الرقمية ، فإذا نتج عن عملية الحساب بيانات غير بيانات البصمة الرقمية المرسلة، فهذا يعني إنه تم العبث بالمحرر، وتستطيع البصمة الرقمية اكتشاف أي تغيير يلحق بالمحرر الرقمي وتتكرر العملية في كل مرة بين المرسل والمرسل إليه .

إن الشروط العامة لقبول المحرر الرقمي[3] كدليل في الإثبات هي قابلية المحرر الرقمي للقراءة وإمكانية الاطلاع عليه وذلك لتبين ماورد به ،[4]والحفاظ علي سلامة بيانات المحرر بما

---

[1] راجع في ذلك : د/ الأنصاري حسن النيداني، القاضي والوسائل الرقمية الحديثة ، مرجع سابق ، ص58 وما بعدها .

[2] راجع في ذلك : محمد جميل إبراهيم ، اثر التقنيات الحديثة في مجال الدليل الكتابي ، مرجع سابق، ص 155 وما بعدها.

[3] راجع في ذلك: د/عبد التواب مبارك ، الدليل الرقمي أمام القاضي المدني ، مرجع سابق ، ص 91 وما بعدها.

[4] راجع في ذلك :

_ https://www.tandfonline.com/doi/full/10.1080/15567280500541462?src=recsys

يحميه من أي تغيير أو تحريف ، و ضمان عدم الاختراق واعتراض المحتوي كدليل رقمي ،[1] و المحرر اذا أصبح رقميا في صورةpdf مثلا فإن هذا لا يضمن الحماية بصورة مطلقة ففي العالم الافتراضي مخاطر أيضا وإن كانت مختلفة من حيث الطبيعة والتقنية المستخدمة، لذا اشترط المشرع الفرنسي في م١ من القانون المدني لقبول الكتابة في الشكل الرقمي أن يكون من الممكن تحديد الشخص الذي صدر عنه، وان تحفظ في ظروف من طبيعتها ضمان سلامة المحرر وهو نفسه موقف المشرع المصري والذي نص علي ذلك في قانون التوقيع الرقمي، وقد ورد في م 11 من اللائحة التنفيذية للقانون[2] ضوابط حماية بيانات المحرر، وهي ذاتها – من حيث المبدأ– ذات الآليات الخاصة بالتوقيع الرقمي.

والهدف الأساسي أن يتم حفظ ملفات القضايا وما يتصل بها من بيانات بحالتها وفي ظروف تضمن لها السلامة والبعد عن أي تحريف أو تغيير، وذلك حتي يضمن الرجوع إليها

---

[1] راجع في ذلك المادة الأولي من جرائم تقنية المعلومات رقم 175 لسنة 2018 والتي وضع بها المشرع تعريفا لكل من الاختراق والاعتراض والمحتوي والدليل الرقمي علي النحو التالي :

– (**الاعتراض** : مشاهدة البيانات أو المعلومات أو الحصول عليها بغرض التنصت أو التعطيل، أو التخزين أو النسخ، أو التسجيل ، أو تغيير المحتوي ، أو إساءة الاستخدام أو تعديل المسار أو إعادة التوجيه وذلك لأسباب غير مشروعة ودون وجه حق) .

– (**الاختراق** : الدخول غير المرخص به ، أو المخالف لأحكام الترخيص ، أو الدخول بأي طريقة غير مشروعة ، إلي نظام معلوماتي أو حاسب آلي أو شبكة معلوماتية، وما في حكمها) .

(المحتوي : أي بيانات تؤدي بذاتها، أو مجتمعه مع بيانات أو معلومات أخري إلي تكوين معلومة أو تحديد توجه أو اتجاه أو تصور أو معني أو الإشارة إلي بيانات أخري) .

– (**الدليل الرقمي** : هو أية معلومات رقمية لها قوة أو قيمة ثبوتية مخزنة أو منقولة أو مستخرجة أو مأخوذة من أجهزة الحاسب أو الشبكات المعلوماتية وما في حكمها ، والممكن تجميعه وتحليله باستخدام أجهزة أو برامج أو تطبيقات تكنولوجية خاصة) .

[2] م ١١ من **اللائحة التنفيذية لقانون التوقيع الرقمي:** (مع عدم الإخلال بما هو منصوص عليه في المواد ٢،٣،٤ يتم من الناحية الفنية ، التقنية كشف أي تعديل أو تبديل في بيانات المحرر الرقمي باستخدام تقنية شفرة المفتاحين (العام والخاص) وبمضاهاة شهادة التصديق الرقمي وبيانات إنشاء التوقيع الرقمي بأصل هذه الشهادة وتلك البيانات أو بأي وسيلة مشابهة) .

في أي وقت سواء أثناء سير القضية، أو في مرحلة الطعن في الحكم، أو حتي لأغراض الحفظ عموما.

و المحررات الرقمية عبارة عن كل رسالة بيانات تتضمن معلومات تنشأ وتدمج أو تخزن أو ترسل أو تستقبل كليا أو جزئيا بوسيلة رقمية أو رقمية أو ضوئية أو بأية وسيلة آخري مشابهة[1].

وهذه البيانات الرقمية تثبت علي دعائم رقمية[2] غير ورقية ذات خواص محددة كالأقراص الممغنطة وذاكرة الحاسب الآلي المثبتة والغير مثبتة أو قد تكون مثبتة علي دعائم رقمية غير مادية من خلال شبكة الإنترنت بما في ذلك البريد الرقمي[3].

وتشمل المحررات الرقمية[4] أيضا السجل الرقمي وهو عبارة عن البيانات التي تنشأ أو ترسل أو تستلم أو تبث أو تحفظ بوسيلة رقمية وتكون قابلة للاسترجاع أو الحصول عليها بشكل يمكن فهمها. **ولقد ايد حكم محكمة النقض[5] الصادر بالطعن12415 لسنة78 ق – جلسة 2018/12/23** حجية المحررات الرقمية في الإثبات حيث ورد بنص الحكم : (كما أنه من

---

1 راجع في ذلك : بدر بن عبدالله الجعفري، بحث بعنوان الإثبات الرقمي في المنازعات التجارية، مقدم للمتلقي العدلي "وسائل الإثبات" الذي نظمته الغرفة التجارية بمدينة الأحساء ، المملكة العربية السعودية، يناير 2013، ص 30.

2 – **دعامة رقمية:** (أي وسيط مادي لحفظ وتداول البيانات والمعلومات الرقمية ومنها الأقراص المدمجة أو الأقراص الضوئية أو الذاكرة الرقمية أو ما في حكمها) . راجع في ذلك المادة الأولي من جرائم تقنية المعلومات رقم 175 لسنة 2018 .

3 راجع في ذلك : أ.د. عابد فايد عبد الفتاح فايد ، القاضي والتنازع بين الأدلة الكتابية التقليدية والرقمية . دراسة مقارنة . بين القانون الفرنسي وقوانين بعض الدول العربية ، المؤتمر العلمي الخامس (الافتراضي) ، كلية الحقوق جامعة السلطان قابوس ، " نظم التقاضي وتحديث قواعد الإثبات "تطوير نظم التقاضي وتحديث قواعد الإثبات" ، ٢٢ ديسمبر ٢٠٢٠ ، ص5 وما بعدها

4 راجع في ذلك : محمد جميل إبراهيم ، اثر التقنيات الحديثة في مجال الدليل الكتابي ، مرجع سابق، ص 149

5 راجع في ذلك : (تاريخ آخر دخول: 2021/1/10)

_ https://www.cc.gov.eg/judgment_single?id=111387601&&ja=270764

المقرر أن النص في الفقرة ب من المادة الأولي من القانون رقم ١٥ لسنة ٢٠٠٤ بتنظيم التوقيع الرقمي وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات علي أن (المحرر الرقمي هو رسالة بيانات تتضمن معلومات تنشأ أو تدمج أو تخزن أو ترسل أو تستقبل كليًا أو جزئيًا بوسيلة رقمية أو ضوئية أو بأية وسيلة أخري مشابهة) ، والمادة ١٥ من ذات القانون (للكتابة الرقمية وللمحررات الرقمية في نطاق المعاملات المدنية والتجارية والإدارية ذات الحجية المقررة للكتابة والمحررات الرسمية والعرفية في أحكام قانون الإثبات في المواد المدنية والتجارية ...) يدل علي أن البيانات التي تنشأ أو تدمج أو تخزن أو ترسل أو تستقبل بوسيلة رقمية أو ضوئية أو بأية وسيلة أخري مشابهة تُعد من قبيل المحررات ولها ذات الحجية المقررة للمحررات الرسمية أو العرفية في أحكام قانون الإثبات في المواد المدنية والتجارية وفي نطاق المعاملات المدنية والتجارية والإدارية.

لما كان ذلك ، وكان البين من الأوراق أن الشركة الطاعنة أقامت الدعوي ضد الشركة المطعون ضدها بطلب الحكم بإعدام البضاعة المصدرة إليها من الشركة المطعون ضدها وإلزامها برد قيمة ثمن البضاعة والتعويض استنادًا لإخلال الشركة المطعون ضدها بالتزامها الذي تم بناءً علي العقد الذي وقع بينهما رقميًا ، وكان الثابت بالأوراق أن الشركة المطعون ضدها أنكرت علاقتها التعاقدية بالشركة الطاعنة بجحدها للمحرر الرقمي المتضمن عقد التوريد محل التداعي بما مقتضاه أن المنازعة علي هذا النحو تستدعي تطبيق أحكام قانون تنظيم التوقيع الرقمي الذي ينظم أحكام المحررات الرقمية كدليل إثبات (

- **التوقيع الرقمي وأهمية في الإجراءات القضائية**[1]:

وضع التوقيع علي مستند يحتوي علي معلومات معينة يعني واقعة **توقيع** ، ويأتي التوقيع في صورة علامة خطية خاصة ومميزة يضعها الموقع وتسمح بتمييز شخص الموقع فتنسب إليه شخصيا دون غيره وتعبر عن إقراره بما جاء في المستند[2]. وعرفت الفقرة الثالثة من المادة الأولي من قانون **التوقيع الرقمي** المصري التوقيع الرقمي بإنه (ما يوضع علي محرر رقمي

[1] راجع في ذلك : د/ الأنصاري حسن النيداني، القاضي والوسائل الرقمية الحديثة ، ص195 وما بعدها .

[2] راجع في ذلك : د. محمد المرسي زهرة ، الحاسب الرقمي ، الإثبات والقانون دراسة حول حجية. مخرجات الحاسب في الإثبات ، مكتبة سعيد عبد الله ، القاهرة ، ١٩٩٢ ، ص ٧٩.

ويتخذ شكل حروف أو أرقام أو رموز أو إشارات أو غيرها ويكون له طابع منفرد يسمح بتحديد شخص الموقع وتميزه عن غيره) .

في بدايات ظهور فكرة التوقيع الرقمي[1] كان التركيز عليها بالأساس لأغراض التجارة الرقمية وعقود البيع الرقمي فنجد قانون الاؤنسيترال النموذجي للتوقيعات الرقمية الصادر عام ٢٠٠١ ، أي أن التوقيع نظراً لما له من أهمية في الإثبات وله أهمية قصوي في الإجراءات القضائية، إذ يجب الاستيثاق من صحة البيانات وما تقرره المحررات، لما لها من أثر علي الإجراءات المتبعة في القضية (الصحة أو البطلان)، وعلي الحكم الصادر من القاضي. لذا يجب ضمان الموثوقية عن طريق نظام قانوني محدد للتوقيع الرقمي وآلية تقنية تضمن تحقق سلامة البيانات .[2]

ويقصد بالموثوقية[3] البيانات التي يتم استقبالها وتتضمن ذات المعلومات التي كانت موجودة بها عند إرسالها، فتصل إلي المرسل إليه (الطرف المستقبل) دون أي تعديل سواء بالإضافة أو الحذف أثناء إرسالها من المرسل إلي المرسل إليه والآلية التي تتحقق بها هي في الأساس التوقيع إذ إنها تضفي علي المحرر نوع من التصديق، ولأغراض الموثوقية يكون التوقيع الرقمي مؤمنًا إذا استوفي الشروط الآتية[4]:

- أن يكون خاص بالموقع وحده

---

[1] راجع في ذلك: د/عبد التواب مبارك ، الدليل الرقمي أمام القاضي المدني ، ص 95 وما بعدها.

[2] من أجل مواءمة تشريعاتها مع المعايير الأوروبية ، اعتمد المشرع الإيطالي في 23 يناير 2002 مرسوم تشريعي (مرسوم) ينقل التوجيه الأوروبي 93/1999 / CE بشأن التوقيع الرقمي. تعتبر الوثيقة الرقمية الآن بمثابة نسخ ميكانيكي بالمعني المقصود في المادة 2702 من كوديس سيفيلوله نفس الصلة كما في الوثيقة المكتوبة بخط اليد. علاوة علي ذلك ، فإن التوقيع الرقمي المرتبط بالمستند الرقمي يعطي نفس التأثير الذي سيكون عليه في العالم الورقي ، بقدر ما يطيع التوقيع شروط التوقيع المتقدمة ويضمنه مزود شهادة معتمد.

[3] راجع في ذلك : د. محمد محمد سادات ، حجية التوقيع الرقمي في الإثبات ، رسالة دكتوراه ، مرجع سابق ، ص ٦٩ .

[4] راجع في ذلك : د/ نور خالد عبد المحسن العبد الرازق ، حجية المحررات والتوقيع الرقمي في الإثبات ، عبر شبكة الإنترنت، رسالة دكتوراه ، ج.عين شمس ، ٢٠٠٩ ، ص ١٩٦ ، وراجع أيضا : راجع في ذلك: د/عبد التواب مبارك ، الدليل الرقمي أمام القاضي المدني ، مرجع سابق ، ص 95 وما بعدها.

- أن يتم إنشائه بوسيلة تقع تحد سيطرة الموقع وحده.
- أن يضمن الكشف عن أي تعديل لاحق في البيانات.

إلي جانب أن التوقيع الرقمي والسرية في تداول كل ما يخص القضية من أوراق خاصة حال إرسالها من المحكمة إلي الخصوم أو العكس بالنظر إلي الإجراءات في الخصومة ذاتها، فإن الوقوف علي حجيتها علي درجة كبيرة من الأهمية لأن من المتصور ان تقدم للمحكمة لغرض الإثبات محررات رقمية وأدلة رقمية.

2. التوقيع الرقمي وآثاره القانونية[1] كدليل رقمي[2] :

يعد التوقيع الرقمي أداة تكنولوجية تسمح بضمان صحة وسلامة المستندات الرقمية. وفقًا للائحة الاتحاد الأوروبي رقم 910/2014 والقانون الإسباني للتوقيع الرقمي 59/2003 (يتألف التوقيع الرقمي من أداة قادرة علي السماح بالتحقق من أصل وسلامة الرسائل المتبادلة من خلال شبكات الاتصالات السلكية واللاسلكية ، مع توفير قواعد لتجنب الرفض أو الطعن في الدليل) بيان دوافع القانون الإسباني 59/2003 بشأن التوقيع الرقمي .

3. ألية ضمان موثوقية[3] التوقيع الرقمي والمحررات الرقمية لضمان حجيتها في الإجراءات القضائية:

يجدر الإشارة إلي أن المشرع المصري في قانون التوقيع الرقمي قد قرر حجية المحررات الرقمية وقبولها في الإثبات علي قدم المساواة مع المحررات الورقية. **وهو ما أيده حكم محكمة**

---

[1] راجع في ذلك: د/عبد التواب مبارك ، الدليل الرقمي أمام القاضي المدني ، المرجع السابق ، ص 91 وما بعدها.

[2] راجع في ذلك: د/عبد التواب مبارك ، الدليل الرقمي أمام القاضي المدني ، المرجع السابق ، ص 70 وما بعدها.

[3] سيكون من الخطأ افتراض أن أدلة الكمبيوتر لا يمكن قبولها إلا من خلال بعض هذه الاستثناءات. ليست كل أدلة الكمبيوتر قابلة للتجربة: يمكن تصنيف بعضها كدليل أصلي أو حتي "حقيقي" ويمكن بعد ذلك قبولها علي نفس أساس الصورة أو التسجيل الشريطي لحادث ما. يعتمد ذلك علي الطريقة التي يعمل بها الكمبيوتر ، وفي بعض الحالات ، علي مدي توفر الشهادات الشفوية الداعمة المتعلقة بإدخال البيانات.

النقض الصادر بالطعن12415 لسنة78 ق – جلسة 2018/12/23 بحجية المحررات الرقمية في الإثبات[1] .

وفي إطار الإجراءات القضائية إذا قام أحد الأشخاص برفع دعوي بتقديم المطالبة القضائية رقميا فإن التوقيع الرقمي هو ما يؤكد صدور هذا التصرف عن هذا الشخص بالذات وإقراره به ونسبته إليه، وبالمثل في إعلان المحكمة (الإعلانات أو الإخطارات اللاحقة لانعقاد الخصومة) لأحد أطراف الخصومة رقميا، أيضا عند إصدار القاضي لمسودة الحكم هل من الممكن أن يغني توقيع القاضي الرقمي عن التوقيع العادي، فضلا عن الاعتراف بكافة هذه الإجراءات فإن" **التوقيع الرقمي المؤمن** " له أهمية قصوي في كل هذه الإجراءات[2].

---

[1] حيث ورد بنص الحكم (كما أنه من المقرر أن النص في الفقرة ب من المادة الأولي من القانون رقم ١٥ لسنة ٢٠٠٤ بتنظيم التوقيع الرقمي وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات علي أن المحرر الرقمي هو رسالة بيانات تتضمن معلومات تنشأ أو تدمج أو تخزن أو ترسل أو تستقبل كليًا أو جزئيًا بوسيلة رقمية أو ضوئية أو بأية وسيلة أخري مشابهة) ، والمادة ١٥ من ذات القانون (للكتابة الرقمية وللمحررات الرقمية في نطاق المعاملات المدنية والتجارية والإدارية ذات الحجية المقررة للكتابة والمحررات الرسمية والعرفية في أحكام قانون الإثبات في المواد المدنية والتجارية ...) يدل علي أن البيانات التي تنشأ أو تدمج أو تخزن أو ترسل أو تستقبل بوسيلة رقمية أو ضوئية أو بأية وسيلة أخري مشابهة تُعد من قبيل المحررات ولها ذات الحجية المقررة للمحررات الرسمية أو العرفية في أحكام قانون الإثبات في المواد المدنية والتجارية وفي نطاق المعاملات المدنية والتجارية والإدارية.

لما كان ذلك ، وكان البين من الأوراق أن الشركة الطاعنة أقامت الدعوي ضد الشركة المطعون ضدها بطلب الحكم بإعدام البضاعة المصدرة إليها من الشركة المطعون ضدها وإلزامها برد قيمة ثمن البضاعة والتعويض استنادًا لإخلال الشركة المطعون ضدها بالتزامها الذي تم بناءً علي العقد الذي وقع بينهما رقميًا ، وكان الثابت بالأوراق أن الشركة المطعون ضدها أنكرت علاقتها التعاقدية بالشركة الطاعنة بجحدها للمحرر الرقمي المتضمن عقد التوريد محل التداعي بما مقتضاه أن المنازعة علي هذا النحو تستدعي تطبيق أحكام قانون تنظيم التوقيع الرقمي الذي ينظم أحكام المحررات الرقمية كدليل إثبات) . راجع في ذلك : https://www.cc.gov.eg/judgment_single?id=111387601&&ja=270764

2 راجع في ذلك : د/أسامة أحمد بدر ، حماية المستهلك في التعاقد الرقمي ، دراسة مقارنة ، دار الجامعة الجديد للنشر ، 2005، ص 20 ، 13 .

إن التركيز علي فكرة الموثوقية والرسمية في الأساس يمكن إجماله في نقطتين أساسيتين[1]:

الأولي: إنه في إطار تطور الإجراءات القضائية والاستعانة بالتكنولوجيا فيها فإن التركيز يكون علي ضرورة التثبت من نسبة الورقة / المحرر إلي من صدر عنه وبمعني آخر إيجاد صلة بين الإجراء والشخص الذي صدر عنه الإجراء والوسيلة لذلك هو "التوقيع الرقمي".[2]

---

[1] أعلنت المحكمة البلجيكية العليا منذ عشر سنوات ما يلي:

{' le juge apprécie la culpabilité du prévenu selon son intime الإدانة؛ il le condamne lorsqu'il a la certitude humaine qu'il s'est rendu coupable du fait mis à sa charge '(Cass، 10 November 1992، Pas، 1992، I، p 1247 .}

ترجمة غير مصرح بها: 'يقدّر القاضي بحرية ذنب المدعي عليه وفقًا لتقديره الشخصي للأدلة ؛ لا يمكن إدانته إلا عندما يكون مقتنعًا بأن المتهم ارتكب فعلًا الجرم الذي حوكم من أجله يتعين علي القاضي أن يزن مدي اعتماده علي الأدلة (خاصة ملاحظاته وبيانات المشتبه فيهم والشهود والخبراء ، وكذلك الوثائق المكتوبة). وراجع في ذلك أيضا : (تاريخ آخر دخول علي الموقع : 22/9/2020)

- قانون الإجراءات الجنائية الفرنسي علي الإنترنت :
- http://www.adminet.com/code/index-CPROCPEL.html
- قانون الإجراءات الجنائية الإيطالي علي الإنترنت :
- http://www.camerapenale-bologna.org/codice_procedura_penale/codice_di_procedura_penale_index.htm#cpbo.

[2] راجع في ذلك أيضا : علي سبيل المثال ، القاعدة 96 (استبعاد الأدلة لعدم وجود موثوقية أو تأثير علي نزاهة المحكمة بالوسائل التي تم الحصول عليها) القاعدة 89 ، الفقرة واو (الأصالة) ، القاعدة 92 مكرر أ (ب) (ب) (موثوقية التنفيذ أدلة المحكمة) ، القاعدة 94 مكرر (الخبراء) ، القواعد الإجرائية وقواعد الإثبات ، المحكمة الجنائية الدولية ليوغوسلافيا السابقة ؛FRE (الولايات المتحدة) المادة السادسة ، التي تحدد أوراق اعتماد الشهود ؛ المادة السابعة ، تحدد مؤهلات الشهود الخبراء وآرائهم ؛ المادة الثامنة ، التي تحدد الاختبارات المتعلقة بالإشاعة خارج بيانات المحكمة المستخدمة في المحكمة ؛ المادة التاسعة ، التي تحدد اختبارات التصديق علي الأدلة.

النقطة الثانية[1]: أيضا في إطار إجرائي نجد ضرورة بيان ماهية الإجراء ذاته بما يوازن بين الضمانات الإجرائية Le contenu d' acte ، والطبيعة الرقمية[2] للوسائل التي يتخذ من خلالها الإجراء وهو ما يوجد له صدد في قانون الإجراءات المدنية الكندي الجديد الصادر في٢٠ فبراير ٢٠١٤ والذي أعتمد التكنولوجيا بصورة ملحوظة في الإجراءات المدنية ، و تناولت م ٩٩ بفقرتها الثلاث هذا الأمر وبصفة خاصة في علاقته بإجراء المطالبة القضائية سواء تم هذا الأخير بإرساله عبر الإنترنت أو تم إيداعه بواسطة المدعي لدي قلم الكتاب مثبت علي دعامة رقمية[3] فحددت في الفقرة الأولي والثانية مضمون الإجراء والبيانات التي يتطلبها من ناحية وهوما يثير شروط المحررات الرقمية [4] وحددت الفقرة الثالثة متطلب التوقيع الرقمي.

---

[1] راجع في ذلك : (تاريخ آخر دخول علي الموقع : 22/9/2020)

_ https://www.tandfonline.com/doi/abs/10.1080/13600860420002235 08?src=recsys&journalCode=cirl20

[2] راجع في ذلك : د/ الأنصاري حسن النيداني، القاضي والوسائل الرقمية الحديثة مرجع سابق ، ص 178 وما بعدها .

[3] وقد عرفت المادة الأولي من قانون 175لسنة 2018 الدعامة الرقمية بانها:

دعامة رقمية: أي وسيط مادي لحفظ وتداول البيانات والمعلومات الرقمية ومنها الأقراص المدمجة أو الأقراص الضوئية أو الذاكرة الرقمية أو ما في حكمها.

[4]Art.99 Alinéa 1 Canadienne NCPC:« L'acte de procédure doit indiquer sa nature، exposer son objet، énoncer les faits qui le justifient، ainsi que les conclusions recherchées. Il doit indiquer tout ce qui، s'il n'était pas énoncé، pourrait surprendre une autre partie ou soulever un débat imprévu. Ses énoncés doivent être présentés avec clarté، précision et concision، dans un ordre logique et être numérotés consécutivement.».

4. موقف المشرع المصري بشأن التوقيع الرقمي[1]:

إن الهدف من دراسة موقف المشرع المصري في هذا الصدد هو ضمان أكبر قدر من الأمان المعلوماتي للتوقيع الرقمي بما يمنع من التبديل أو التزوير في بيانات المحرر المذيل بالتوقيع الرقمي، عندما قام المشرع المصري بتنظيم أحكام التوقيع الرقمي بموجب القانون الصادر في ٢٠٠٤ فقد أخذ بمبدأ الحياد التكنولوجي (بمعني ألا يتطلب القانون إلزاما باستخدام تكنولوجيا معينة في التوقيع الرقمي تاركا للمتعاملين باستخدام التوقيع الرقمي حرية اختيار التكنولوجيا المناسبة لهم في إطار معاملتهم الخاصة)[2] ويتبدى ذلك من ان المشرع ذكر دائما التوقيع الرقمي دون تخصيص أو ربط بنوع معين، وهو ما يقودنا إلي إن أنواع التوقيع الرقمي [3] وتحديد نوع التوقيع المعتمد علي درجة عالية من الأهمية لأن أثره القانوني يتحدد بقوة الاتصال بين أدوات التوقيع والوثيقة التي سيتم توقيعها والقدرة علي حماية الوثيقة من أي تلاعب، وتنقسم صور التوقيع علي هذا النحو علي أساس درجة الأمان التي يتيحها كل توقيع إلي[4]:

أ. التوقيع بالنقر علي لوحة المفاتيح

ب. التوقيع بواسطة الرقم السري ، والبطاقة الممغنطة.

ج. التوقيع عن طريق قياس الخواص الحيوية لجسم الإنسان (بصمة الصوت ، بصمة العين ،بصمة الأسنان).

د. التوقيع الرقمي

---

[1] راجع في ذلك : د/ الأنصاري حسن النيداني، القاضي والوسائل الرقمية الحديثة ، مرجع سابق ، ص47 وما بعدها .

[2] وقد أخذت بذات المبدأ الولايات المتحدة وإنجلترا، راجع د. محمد محمد سادات ، المرجع السابق ، ص ٩٦

[3] راجع في ذلك : د./عيسي غسان عبد الله الربضي ، القواعد الخاصة بالتوقيع الرقمي ، رسالة دكتوراه، ج.عين شمس ، ص ٥٧ وما بعدها.

[4] راجع في ذلك: د/عبد التواب مبارك ، الدليل الرقمي أمام القاضي المدني ، دار النهضة العربية ، بدون سنة نشر ، ص 74 وما يليها.

إلا إنه بالرجوع إلي نصوص اللائحة التنفيذية لقانون التوقيع الرقمي والمذكرة الإيضاحية نري أن المشرع اقتصر علي ذكر صورة واحدة هي "**التوقيع الرقمي**" ،[1]كما إن كافة الضوابط التقنية التي اشترطها في الاعتراف بالتوقيع لا يحققها إلا التوقيع الرقمي[2] علي نحو ما سيلي بيانه وما يهمنا في هذا الصدد هو التوقيع الرقمي والذي نوصي بأن يقرر المشرع صراحة اعتماده كوسيلة للتوقيع الرقمي في اطار الإجراءات القضائية فخلافا للمعاملات الخاصة تتعلق إجراءات التقاضي بالنظام العام لاتصالها بتنظيم مرفق القضاء وان يتم ذلك التقرير صراحة دون حاجة إلي أن يستشف من اللائحة التنفيذية[3] .

والتوقيع الرقمي هو أكثر صور التوقيع الرقمي ضمانا لأمن وسلامة البيانات ،[4]ويعتمد التوقيع الرقمي علي التشفير[5] الذي يحمي صحة وأصالة البيانات، فعن طريق التشفير يتم تحويل الرسائل إلي أشكال غير مفهومة ثم إعادتها إلي أشكالها الأصلية ، ويعبر عن التوقيع الرقمي

---

[1] راجع في ذلك : د/ يوسف احمد النوافلة ، رسالة دكتوراه بعنوان "الإثبات الرقمي" ، كلية الحقوق ، جامعة الإسكندرية ، 2010 ، ص62 وما يليها.

[2]راجع في ذلك : د./ محمد محمد سادات ، حجية التوقيع الرقمي في الإثبات ، رسالة دكتوراه ، مرجع سابق ، ص ١٠٨ وما بعدها. وهو ما يتضح من١١ من اللائحة وفي مجموعة فإنها تشترط ضرورة توافر تقنية المفتاح ، ١٠ ،٩ ، المواد ٧ العام والخاص وارتباط استخدام تلك التقنية بشهادة تصديق رقمي . وهو ما يمثل الدالة المبعثرة وهي تقنيات لا تستخدم إلا مع التوقيع الرقمي .

[3] يري جانب من الفقه – وبحق– انه لا يمكن القول بصورة جازمة أن المشرع المصري تراجع عن مبدأ الحياد التكنولوجي وتبني نظام التوقيع الرقمي دون غيره لوجود صور آخري للتوقيع الرقمي موجودة في العمل كالبطاقات الممغنطة، إلا أن الهدف أن المشرع المصري يولي اهتمام بالتوقيع الرقمي باعتباره الصورة التي تضمن أكبر قدر من الحماية والأمن المعلوماتي للتوقيع الرقمي. راجع في ذلك : راجع د. محمد محمد سادات ، حجية التوقيع الرقمي في الإثبات ، رسالة دكتوراه ، المرجع السابق ، ص ١١٣–١١٩ .

[4] يقصد بمصطلح سلامة البيانات: (التحقق من أن البيانات التي تضمنتها الوثيقة لم يحدث بها أي تعديل أو حذف سواء لأسباب طبيعية أو عمدية) . راجع في ذلك : د./ محمد محمد سادات. حجية التوقيع الرقمي في الإثبات ، رسالة دكتوراه ، مرجع سابق ، ص ١٩٥.

[5]راجع في ذلك : د/ يوسف احمد النوافلة ، رسالة دكتوراه بعنوان "الإثبات الرقمي" ، مرجع سابق ، ص88

الذي يعتمد علي التشفير وشهادة التصديق[1] "بالتوقيع الرقمي المتقدم" وقد تطلب المرسوم الصادر من مجلس الدولة الفرنسي رقم ٢٧٢ لسنة ٢٠١٠ بخصوص تطبيق نصوص التوقيع الرقمي، إنه لكي يصدق علي التوقيع وصف "المتقدم" أن يستوفي عدة شروط أن يكون التوقيع خاص بالموقع ويتم إنشائه بوسائل تقع تحت سيطرته ورقابته الخاصة، وان يتم التثبت من أن التوقيع يقوم علي استخدام شهادة رقمية مؤهلة [2] ، وهو نفس موقف المشرع المصري، وباستيفاء تلك المتطلبات يمكن القول أن التوقيع الرقمي والمحرر يعترف بهم القانون ويتمتعوا بأقصى قدر من الأمان[3].

---

[1] راجع في ذلك : د/ يوسف احمد النوافلة ، رسالة دكتوراه بعنوان "الإثبات الرقمي" ، مرجع سابق ، ص90 وما بعدها.

[2] راجع في ذلك:

Art. 1/ 2 : « Signature électronique sécurisée : une signature électronique qui satisfait، en outre، aux exigences suivantes –être créée par des moyens que le signataire puisse garder sous son être propre au signataire –garantir avec l'acte auquel elle s'attache un lien tel que toute، contrôle exclusif; modification ultérieure de l'acte soit détectable

https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT00 0000404810 last visited 22 October 2017 .

[3] وما يتكفل بضمان تحقيق ذلك أيضا بجانب كل ما سبق اذا ما تعدي شخص واتلف محرر او دليل رقمي فأنه يطبق عليه المادة 17 من قانون 175 لسنة 2018 الخاص بجرائم تقنية المعلومات والتي تنص علي :

جريمة الاعتداء علي سلامة البيانات والمعلومات والنظم المعلوماتية

(يعاقب بالحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن100 ألف جنيه ولا تجاوز 500 ألف جنيه، أو بأحدي هاتين العقوبتين كل من أتلف أو عطل أو عدل مسار أو ألغي كلياً أو جزئياً، متعمداً وبدون وجه حق، البرامج والبيانات أو المعلومات المخزنة، أو المعالجة، أو المولدة أو المخلقة علي أي نظام معلوماتي وما في حكمه، أيا كانت الوسيلة التي استخدمت في الجريمة) .

ثانيا : الرسائل النصيةSMS))[1]:

تثير الرسائل النصية التي ترسلها أجهزة الهواتف المحمولة (اللاسلكية) التساؤل حول إمكانية قبولها كدليل في الإثبات .

وقد قبلت محكمة النقض الفرنسية في حكمها الصادر بتاريخ 23/5/2007 الرسائل النصية كدليل في الإثبات، ولكن بشرط أن يكون الحصول عليها قد تم بطريقة لا خداع فيها .

وقد اعتد المشرع المصري برسائل البريد العادي كدليل للإثبات وفقا لنص المادة (16) من قانون الإثبات، وقد سوي المشرع بينها وبين المحررات العرفية في الإثبات، فالرسالة وإن لم يقصد بها أن تكون دليلا كتابيا فإنها تعد كذلك ما دامت موقعا عليها، وقد تكون حجة علي المرسل بصحة المدون فيها إلي أن يثبت العكس بالطرق المقررة قانونا للإثبات .

فإذا لم يكون موقعا عليها من المرسل فإنها تعتبر مبدأ ثبوت بالكتابة متي كانت مكتوبة بخطه أما إذا لم تكن بخطه فلا قيمه لها في الإثبات .

أما بالنسبة للرسائل النصية[2] الصادرة من الهواتف المحمولة (SMS) فإنها دائما وأبدا لا تكن موقعه من مرسلها وبالتالي فإنه فيما يتعلق بهوية كاتب أو مرسل الرسالة النصية فإنه من حيث المبدأ يمكن القول بأن الرسالة النصية تعد صادرة من قبل صاحب الخط الهاتفي الذي تم إرسال هذه الرسالة منه إلا إذا ثبت غير ذلك، ذلك أن صاحب الخط هو الذي لجأ بداية إلي المشغل للخطوط الخلوية واقتني أو ملك خط الهاتف الذي من خلاله تم إرسال الرسالة النصية.

---

[1] راجع في ذلك : د/ أحمد محمد عبدالرحمن، "نظرة حول نظام التقاضي الرقمي في مصر" ، مرجع سابق ، ص 24 .

2 راجع في أمن الرسائل الفورية :

https://docplayer.net/680438-Instant-messaging-security.html

ثالثا : الإثبات بالبريد الرقمي[1]:

تعد رسائل البريد الرقمي[2] ضمن الوسائل الحديثة التي تصلح كدليل في الإثبات[3]. وكما سبق وأشرنا فإنه لا بد من التأكد من هوية الشخص المرسل، وفي هذا الصدد فإنه لابد من الإشارة إلي أن البريد الرقمي لا يمكن أن يكون دليلا كافيا لإثبات هوية المرسل لذلك لابد من إضافة ما يفيد ويؤكد هذه الجهة المرسلة وذلك من خلال مركز الخدمات التقنية للاتصالات الذي يقوم بدور توزيع البريد الرقمي ، ويمكن اشتراط أن تكون رسالة البريد الرقمي موقعه من مرسلها حتي يمكن الاعتداد بها كوسيلة من وسائل الإثبات.

وأخيرا فإنه لكي تقوم الكتابة الرقمية مكان الكتابة التقليدية في مجال الإثبات فإنه يجب أن تكون هذه الكتابة قابلة للقراءة أولا حتي يتم التعرف علي محتوي المحرر وأن تكون هذه الكتابة غير قابلة للتعديل حتي لا يغير أحد الأطراف محتواها دون علم الطرف الآخر وأن يتم حفظ هذه المحررات حتي يتم الرجوع إليها عند الحاجة لذلك[4].

- **حجية البريد الرقمي في الإثبات[5]:**

لقد كانت الكتابة علي الورق هي الأصل الغالب، إلا أن المحرر لم يكن في أي وقت مقصورًا علي ما هو مكتوب علي ورق وحده، وكل ما يتطلبه المشرع للإثبات هو ثبوت نسبة

---

[1] راجع في ذلك : د/ أحمد محمد عبدالرحمن، "نظرة حول نظام التقاضي الرقمي في مصر" ، مرجع سابق ، ص 24 .

[2] – البريد الرقمي : (وسيلة لتبادل رسائل رقمية علي عنوان محدد ، بين أكثر من شخص طبيعي أو اعتباري ، عبر شبكة معلوماتية ، أو غيرها من وسائل الربط الرقمية، من خلال أجهزة الحاسب الآلي وما في حكمها) . المادة الأولي من قانون تقنية المعلومات رقم 175 لسنة 2018 .

[3] راجع في ذلك : د/ يوسف احمد النوافلة ، رسالة دكتوراه بعنوان "الإثبات الرقمي" ، مرجع سابق ، ص126 وما بعدها.

[4] راجع في ذلك : د. محمد محمد سادات. حجية التوقيع الرقمي في الإثبات ، رسالة دكتوراه ، ج. المنصورة ، ٢٠١٠ ، ص ١٩٥ .

[5] راجع في ذلك : د/ يوسف احمد النوافلة ، رسالة دكتوراه بعنوان "الإثبات الرقمي" ، مرجع سابق ، ص 129 وما بعدها وراجع أيضا : راجع في ذلك : د/ الأنصاري حسن النيداني، القاضي والوسائل الرقمية الحديثة ، مرجع سابق ، ص99 وما بعدها .

المحرر إلي صاحبه، فلا ارتباط قانونًا بين فكرة الكتابة والورق، ولذلك لا يُشترط أن تكون الكتابة علي ورق بالمفهوم التقليدي ومذيلة بتوقيع بخط اليد، وهو ما يوجب قبول كل الدعامات الأخرى – ورقية كانت أو رقمية أو أيًا كانت مادة صنعها – في الإثبات. البريد الرقمي – e) mail) هو وسيلة لتبادل الرسائل الرقمية بين الأشخاص الذين يستخدمون الأجهزة الرقمية من أجهزة كمبيوتر أو هواتف محمولة أو غيرها، تتميز بوصول الرسائل إلي المرسل إليهم في وقت معاصر لإرسالها من مُرسِلها أو بعد برهة وجيزة، عن طريق شبكة المعلومات الدولية (الإنترنت) أيًا كانت وسيلة طباعة مستخرج منها في مكان تلقي الرسالة، وسواء اشتملت هذه الرسائل علي مستندات أو ملفات مرفقة Attachments أم لا. ولقد أجازت القوانين الوطنية والاتفاقيات الدولية للقاضي استخلاص واقعتي الإيجاب والقبول – في حالة التعاقد الرقمي – من واقع تلك الرسائل الرقمية دون حاجة لأن تكون مفرغة كتابيًا في ورقة موقعة من طرفيها، ذلك أن هذه الرسائل يتم تبادلها عن طريق شبكة المعلومات الدولية (الإنترنت)، ولذلك فإن أصول تلك الرسائل – مفهومة علي أنها بيانات المستند أو المحرر الرقمي – تظل محفوظة لدي أطرافها – مهما تعددوا – المُرسِل والمُرسَل إليهم داخل الجهاز الرقمي لكل منهم، فضلًا عن وجودها بمخزنها الرئيسي داخل شبكة الإنترنت في خادمات الحواسب Servers للشركات مزودة خدمة البريد الرقمي للجمهور. وفي كل الأحوال، فإنه في حالة جحد الصور الضوئية، فلا يملك مُرسِل رسالة البريد الرقمي أن يقدم أصل المستند أو المحرر الرقمي، ذلك أن كل مستخرجات الأجهزة الرقمية، لا تعدو أن تكون نسخًا ورقية مطبوعة خالية من توقيع طرفيها، ومن ثم فإن المشرع وحرصًا منه علي عدم إهدار حقوق المتعاملين من خلال تلك الوسائل الرقمية الحديثة حال عدم امتلاكهم لإثباتات مادية علي تلك المعاملات، قد وضع بقانون تنظيم التوقيع الرقمي ولائحته التنفيذية الضوابط التي تستهدف التيقن من جهة إنشاء أو إرسال المستندات والمحررات الرقمية وجهة أو جهات استلامها وعدم التدخل البشري والتلاعب بها للإيهام بصحتها، ولا يحول دون قبول الرسالة الرقمية كدليل إثبات مجرد أنها جاءت في شكل رقمي، ولهذا فإنها تكون عصية علي مجرد جحد الخصم لمستخرجاتها وتمسكه بتقديم أصلها؛ إذ إن ذلك المستخرج ما هو إلا تفريغ لما احتواه البريد الرقمي، أو الوسيلة الرقمية محل التعامل، ولا يبقي أمام من ينكرها من

سبيل إلا طريق وحيد هو المبادرة إلي الادعاء بالتزوير وفق الإجراءات المقررة قانونًا تمهيدًا للاستعانة بالخبرة الفنية في هذا الخصوص.

ونظرا للتطور الهائل والسريع في المعاملات وانتشار شبكة الإنترنت وتزايد استخدام البريد الرقمي في المعاملات التجارية والتصرفات القانونية أصبح من الضروري الوقوف علي معالجة حجية البريد الرقمي في الإثبات من حيث الفرضان التاليان:

الأول : حجية البريد رقمي (**الرسمي /غير الرسمي**) غير الموقع .

الثاني :حجية البريد رقمي (**الرسمي / غير الرسمي**) المذيل بالتوقيع .

الفرض الأول : البريد الرقمي (الرسمي /غير الرسمي) غير الموقع[1]

ويقصد به البريد التقليديe-mail والذي يستخدم في الحياة اليومية وتختلف حجيته بحسب الأحوال والمجال الذي يستخدم فيه وعما اذا كان يستخدم في المعاملات التجارية أو المدنية وذلك علي النحو التالي.

- **حجية البريد الرقمي في المواد المدنية والتجارية والمختلطة:**

فيما يتعلق بالمواد التجارية يأخذ المشرع الفرنسي بمبدأ حرية الإثبات وكذلك المشرع المصري في شان المعاملات التجارية أيا كانت قيمتها وفي شان التصرفات المدنية التي لا تزيد قيمتها علي ألف جنية لا غير حيث يمكن إثباتها بأي طريق من طرق الإثبات بما في ذلك البينة والقرائن[2] ولا يتقيد بالدليل الكتابي وهو ما أكده نص المادة 1/69 من قانون التجارة رقم 17 لسنة 1999 .[3] وأقره المشرع المصري بحكم محكمة النقض المصرية **بالطعن رقم**

---

[1] راجع في ذلك : د/ يوسف احمد النوافلة ، رسالة دكتوراه بعنوان "الإثبات الرقمي" ، مرجع سابق ، ص 129 وما بعدها.

[2] **تعرف القرينة بوجه عام** : (بأنها استنباط أمر مجهول من أمر معلوم لذلك تعد من أدلة الإثبات غير المباشر لأن الإثبات فيها لا يقع علي الواقعة ذاتها مصدر الحق وإنما علي واقعة أخري إذا ثبتت أمكن أن نستدل من خلالها علي ثبوت الواقعة المرتبة للأثر القانوني المتنازع فيه) ، راجع في ذلك : **د/ سحر عبد الستار إمام** ، دور القاضي في الإثبات دراسة مقارنة، دون ناشر،2002، ص 315.

[3] علي انه ((يجوز إثبات الالتزامات التجارية أيا كانت قيمتها بكافة طرق الإثبات مالم ينص القانون علي غير ذلك)) ، كما نصت الفقر 2 من نفس المادة علي انه ((فيما عدا الحالات التي يوجب فيها القانون الإثبات

17689 لسنة 89 قضائية (الدوائر التجارية – جلسة10/3/2020) بحجية الرسائل الرقمية في الإثبات ، وانه لا يجوز جحدها وطلب تقديم أصولها بل يجوز فقط المبادرة إلي الادعاء بتزويرها ، وما أقره أيضا بالطعن رقم ١٧٠٥١ لسنة ٨٧ قضائية (الدوائر التجارية – جلسة 2019/03/28)[1] .

الفرض الثانى : حجية البريد الرقمي المذيل بتوقيع رقمي[2]

وفي اطار التحول إلي الرقمية في كافة المجالات والأنشطة، ولمواكبة التطور الهائل في ظل الثورة الصناعية الرابعة فالتفكير في تطبيق تكنولوجيا التوقيع الرقمي بصوره[3] والذي تكمن

بالكتابة فالمواد التجارية يجوز فيها إثبات عكس ما اشتمل علي دليل كتابي أو أثباتها يجاوز هذا الدليل بكافة الطرق)) ، غير انه اشترط للاستفادة من مبدا حرية الإثبات في المواد التجارية يجب أن يكون التصرف تجاريا وبين تجار وبناءا علي ذلك فانة في نطاق التصرفات والمعاملات التجارية القائمة علي مبدا حرية الإثبات يمكن اعتبار رسالة البريد الرقمي قرينة قضائية للإثبات وجود التصرف وجود التصرف عبر شبكة الأنترنت حتي لو زادت قيمة التصرف عن النصاب القانوني المقرر للإثبات بالبينة وهو خمسمائة جنية إذ أن الأمر يخضع في جميع الأحوال الي سلطة القاضي .

• أما في المواد المختلطة والذي يكون فيها احد طرفيها تاجر يتعاقد لأغراض تجارية والطرف الأخر ليس تاجرا ويتعاقد لأغراض شخصية أو عائلية فلا يستفاد من حرية الإثبات إلا غير التاجر حين يتقيد التاجر بطرق الإثبات المدنية.

وعلي ذلك يمكن مثلا للمستهلك الذي يتعاقد مع تاجر عبر شبكة الإنترنت أن يتمسك بالبريد الرقمي في الإثبات باعتباره قرينة قضائية أما التاجر فلا يكون أمامه قبل المستهلك إلا اتباع القواعد المدنية في الإثبات بحيث يلتزم بالإثبات كتابة اذا زادت قيمة التصرف عن خمسمائة جنية ومن ثم يمتنع أن يتمسك برسالة البريد الرقمي في الإثبات.

[1] راجع في ذلك :

– https://www.cc.gov.eg/judgment_single?id=111398859&ja=275421

[2] راجع في ذلك : د/ يوسف احمد النوافلة ، رسالة دكتوراه بعنوان "الإثبات الرقمي" ، مرجع سابق ، ص 130 وما بعدها .

[3] راجع في ذلك : أيمن سعد عبد المجيد سليم ، التوقيع الرقمي ، دراسة مقارنة ، دار النهضة العربية ، 2005، ص26 وما بعدها .

أهميته في زيادة مستوي الأمن والخصوصية[1] في التعاملات نظرا لقدرة هذه التقنية علي حفظ سرية المعلومات[2] والرسائل المرسلة وعدم قدرة أي شخص آخر علي الاطلاع أو تعديل أو تحريف الرسالة كما يمكن تحديد هوية المرسل والمستقبل رقميا للتأكد من مصداقية الشخصين . وهو ما أقره المشرع المصري بالحكم الصادر من محكمة النقض[3] في **الطعن رقم ١٢٤١٥ لسنة ٨٧ قضائية (الصادر بجلسة 23/12/2018)** . حيث اقر بحجية المحرر الرقمي الموقع بعقد رقمي.

ولعل هذا هو ما دفع الأمم المتحدة متمثلة في لجنة القانون التجاري الدولي الاونيسترال unicitral إلي إصدار النموذج للتجارة الرقمية سنة 1996 والقانون النموذجي بشان التوقيع الرقمي الصادر سنة 2001 ومعاهدة استخدام وسائل الاتصال الرقمية في العقود الدولية وإضفاء الحجية القانونية عليها كما أصدر الاتحاد الأوروبي التوجيه الأوروبي القانون رقم 93/1999 في 13 ديسمبر 1999 في شان التوقيع الرقمي وذلك الزم الدول الأعضاء بنقل مضمونة داخل تشريعاتهم الوطنية في خلال 18 شهر كما أصدرت عدة دول قوانين التوقيع الرقمي ومنها :((أمريكا / إنجلترا / سنغافورة / مصر/ الإمارات / الأردن / تونس / الجزائر / البحرين)) .

ولعل السبب في ثقة المتعاملين عبر الإنترنت والمتمثلة في اللجوء إلي التوقيع الرقمي[4] وجود طرف ثالث أو وسيط مقبول وموثوق فيه وهو طبقا للقانون المصري هيئة صناعة

---

[1] راجع في ذالك : د/ فاطمة عادل سعيد ، "التقاضي عبر وسائل التكنولوجيا والاتصال الحديث " ، مرجع سابق ، الجزء الأول ، ص 396 ، وراجع أيضا :

Zheng, Tina, "Advanced Surveillance Technologies: Privacy and Evidentiary Issues" (2016). Cornell Law School J.D. Student Research Papers. 37, p1-10, http://scholarship.law.cornell.edu/lps_papers/37

[2] راجع في ذلك : د. علي بن سعيد بن حمود البداعي ، التقاضي عن بعد ، مرجع سابق ، ص12 .

[3] راجع في ذلك :

_ https://www.cc.gov.eg/judgment_single?id=111387601&&ja=270764

[4] التحقق من ان البيانات التي تضمنتها الوثيقة لم يحدث بها أي تعديل أو حذف سواء لأسباب طبيعية أو عمدية." راجع في ذلك : د. محمد محمد سادات. حجية التوقيع الرقمي في الإثبات ، مرجع سابق ، ص ١٩٥ .

تكنولوجيا المعلومات وهو ما دفع البعض يسال عن نوع المحرر المكتوب الذي يشكله البريد الرقم هل هو رسمي أم عرفي ؟؟؟

وللإجابة عن هذا التساؤل يجب أولا أن نرجع إلي تعريف المحرر الرسمي والعرفي وشروطه وفق قانون الإثبات المصري والذي عرف المحرر الرسمي بإنه[1]: ((المحرر الذي يصدر عن موظف عام او شخص مكلف بأداء خدمة عامة وذلك في حدود سلطته واختصاصه وطبقا للأوضاع القانونية لتوثيق الأوراق الرسمية)) كما عرف المحرر العرفي بإنه ((المحرر الذي يتم بين الأفراد طبقا للعادات دون تدخل من موظف رسمي)) المادة 14 إثبات.

ولكن المشرع لم يتعرض لمعالجة البريد الرقمي الرسمي بالهيئات الحكومية والمعاملات المدنية والتجارية به ولم يطرح معالجات لها.

فلو افترضنا أن البريد الرقمي الرسمي هو في نفس مكانة المحرر الرسمي لوجب علينا إعمال القياس في كافة المعاملات التي ستجري به كما لو كان محرر رسمي.

ولكن الفرض السابق يفتقر الي ضوابط يتم بها تمييز البريد الرسمي من غير الرسمي في المعاملات ، وما هي حدود وسلطات المالك للبريد الرسمي وحجيته في مواجهته وكل من يتعامل معه . والآثار القانونية الناتجة عن استخدامه في محله وفي غير محله . وهل يتساوى البريد الرسمي في الحجية مع البريد الموقع توقيع رقمي في الإثبات حتي ولو لم يتم توقيعه[2] .

---

1 وللمزيد حول المحرر الرسمي والعرفي وشروطه راجع في ذلك :

العالم الفقيه :ا.د/ عبد الرازق السنهوري ، الوسيط في شرح القانون المدني ، الجزء الثاني ، نظرية الالتزام بوجه عام ، طبعة 2004 ، ص 97 ، وما بعدها ، وراجع أيضا : عبد المنعم فرج الصدة ،الإثبات في المواد المدنية ، مكتبة مكتبة مصطفي البابي الحلبي بمصر، 1954، ص78 وما بعدها ، وراجع أيضا: جميل الشرقاوي، الإثبات في المواد المدنية ، دار النهضة العربية ،1976 ،ص41 وما بعدها ، سمير عبد السيد تناغو ، النظرية العامة في الإثبات ، منشأة المعارف بالإسكندرية ، 1999، ص131 وما بعدها .

2 راجع في ذلك : محمد حسين منصور ، الإثبات التقليدي والرقمي ، دار الفكر الجامعي بالإسكندرية ،2006 ،ص 57 وما بعدها .

وبناءا علي ما سبق تعتبر الرسالة الرقمية بالبريد غير الرسمي التي تحمل توقيعا لصاحبها محرر عرفي في مجال الإثبات[1] .

أما مقدم خدمة التوثيق فتنحصر وظيفته في إصدار الشهادات والتصديق لمن يطلبها.

- **حجية البريد الرقمي الموصي به[2] :**

عرف التوجيه الأوروبي الصادر في 15 ديسمبر 1997 يشان القواعد التي تحكم تنمية السوق الداخلي للخدمات البريدية وتحسين جودتها في المادة 2/9 منة البريد الموصي عليه إنه ((خدمة تتم وفق إجراءات تكفل ضمان الإرسال ضد مخاطر الفقد أو السرقة أو التلف وتوفي للمرسل لقاء مبلغ جزافي يدفعه)).

ووفقا للقانون المصري نجد امثله علي البريد الموصي به كما في حالة الأعذار إذ يجب علي الدائن قبل أن يشرع في التنفيذ العيني أن يعذر مدينه ويكون ذلك بأنذاره أو ما يقوم مقام الإنذار عملا بنص المادة 219 مدني كما قد أورد القانون أحيانا استخدام البريد الموصي به كما في حالة الإعلان القضائي .

ويمكن تطبيق ذلك علي البريد الرقمي الموصي به بشرط وجود علاقه بين أشخاص ثلاثة ((المرسل والمرسل إليه ومقدم الخدمة)) ، حيث يقوم الراسل بتعيين هويته لدي مقدم الخدمة والذي يقوم بدور مصلحه البريد وذلك أما باختيار اسم دخول وكلمه مرور سريه أو أن يحصل علي شهاده مصدق عليها من موثق الخدمة أو مقدمها وهذا الاختيار يبلغ للمرسل إليه ثم يضغط الأخير علي أيقونة فيتم تحميل الرسالة عندئذ يقوم مقدم الخدمة بإرسال علم الوصول إلي المرسل إليه مبينا ساعته وتاريخه وساعه الاطلاع علي الرسالة ووفق هذا التصور فان

---

[1] وهو ما أكد عليه أحكام محكمة النقض المصرية التالية :

- الطعن رقم 17689لسنة 89 قضائية الدوائر التجارية – جلسة 10/3/2020.
- الطعن رقم 17051 لسنة 87 قضائية الدوائر التجارية – جلسة 28 /3/2019.
- الطعن رقم 12415 لسنة 87 قضائية الدوائر التجارية – جلسة 23/12/2018.

[2] راجع في ذلك : د. عيسي غسان عبد الله الربضي ، القواعد الخاصة بالتوقيع الرقمي ، رسالة دكتوراه، ج.عين شمس ، ص ٥٧ وما بعدها.

البريد الرقمي الموصي عليه يقدم نفس دور البريد التقليدي بل إنه افضل منه لإنه يحمل ما يفيد اطلاع المرسل إليه علي الرسالة ووقت حدوث ذلك بعكس التقليدي.

ومن اجل ذلك تدخل المشرع الفرنسي بالقانون الصادر في 21 يونيه 2004 الخاص بالثقة في الاقتصاد الرقمي والذي اعطي الحكومة سلطه إصدار الأوامر الخاصة بتعديل النصوص المطبقة لهدف الوصول إلي أبرام العقود بالطريق الرقمي واعملا لذلك فقد صدر المرسوم رقم 674/2005 في 16 يونيو 2005 والذي سمح بإتمام بعض الشكليات التي يستلزمها القانون بطريق رقمي وأصبح البريد الرقمي معترفا به في المادة 1369/8 من القانون المدني علي ((الخطاب الموصي عليه والخاص بإبرام العقد او تنفيذه يمكن إرساله بالبريد الرقمي)) .

ومن جانبنا نري الأخذ بالرأي القائل بأن عنوان البريد الرقمي عبارة عن موطن افتراضي للأشخاص سواء الطبيعية أو الاعتبارية علي شبكة الإنترنت ، فالشخص عندما يقوم بتسجيل عنوان رقمي باسمه علي شبكة الإنترنت يكون قد اختار مقرا قانونيا ترتبط به مصالحه ويباشر من خلاله نشاطا يتمثل في نشر بياناته الخاصة وأسراره الشخصية وهواياته وغيرها من الأعمال ومن ضمنها مراسلاته لجميع الجهات المحلية والدولية .

ويعد هذا الموطن افتراضيا وليس موطنا حقيقيا وبالتالي فإنه يمكن استخدامه كالموطن المختار المنصوص عليه في قانون المرافعات في نطاق إعلان الأوراق القضائية المراد إيصالها إلي علم صاحب هذا العنوان الرقمي باعتباره "الموقع الرقمي المختار ،[1]"إلا إنه لا يمكن استخدامه في تحديد المحكمة المختصة بنظر النزاع حيث إنه يربط الشخص دون تحديد للمكان فهو يحدد فقط مقدم الخدمة علي شبكة الإنترنت وبالتالي يجب عند تحديد المحكمة المختصة بنظر النزاع الاستعانة بالموطن الحقيقي للأشخاص وليس الموطن الافتراضي .

[1] هذا وقد نصت المادة 13 من قانون 146 لسنة 2019 بتعديل بعض أحكام قانون المحاكم الاقتصادية الصادر بالقانون رقم 120 لسنة 2008 علي تحديد المقصود بالعنوان الرقمي المختار بانه:
(الموطن الذي تحدده الجهات والأشخاص المبينة بهذا القانون لإعلانهم بكافة إجراءات الدعاوي المقامة رقميا سواء تمثل في بريد رقمي خاص بهم أو رقم هاتف أو غيرها من الوسائل التكنولوجية . وهو ما يمكن القياس عليه والاستئناس به في مجال إجراءات التقاضي الرقمي امام القضاء المدني) .

ويجب في هذه الحالة إسباغ الحماية المدنية والجنائية علي هذا الموطن الافتراضي وإجبار الغير علي احترام الحياة الخاصة بهذا الموطن ومراعاة الحقوق والحريات الرقمية المتصلة به .

و بعد كل ما تقدم تري الباحثة إنه لزاما علي المشرع المصري أن يتدخل بتعديل تشريعي ينظم البريد الرقمي الموصي عليه بشكل دقيق ومنظم ويبين حجيته القانونية وقوته الثبوتية لاسيما مع تزايد استخدام البريد الرقمي في معظم التعاملات سواء المدنية أو التجارية .

رابعا: الإثبات بالتسجيلات الرقمية (المسموعة والمرئية)[1]

وهي التسجيلات التي يتم ضبطها وتخزينها بواسطة الآلة الرقمية ويقصد بها تسجيل المحادثات الهاتفية سواء صوتيا أو فيديو وسواء أكانت هاتفيا أو علي الإنترنت من أحد الأطراف .

ولقد ثار خلاف بين الفقه حول شرعية استعمال التسجيل الصوتي كدليل إثبات وانقسموا إلي عدة آراء منهم من يؤيد الأخذ بهذه الوسيلة في الإثبات بصفة مطلقة ومنهم من يعارض الأخذ بها ومنهم من يحيط هذا الدليل بشروط معينة ومنهم من يجيز التسجيلات الصوتية إذا كان التسجيل مقدما للتدليل علي براءة المتهم ولو كان الحصول عليه بطريق غير مشروع[2].

ولقد حسم المشرع في قانون الإجراءات الجنائية الأمر فأجاز إجراء تسجيلات لأحاديث جرت في مكان خاص متي كان لذلك فائدة في ظهور الحقيقة ولقد ربط ذلك بشروط معينة هي أن يكون هذا الحديث له فائدة في ظهور الحقيقة وأن يكون في جناية أو جنحة معاقب عليها بالحبس لمدة تزيد علي ثلاثة أشهر ويجب أن يكون هذا التسجيل بناء علي أمر مسبب ولمدة لا

---

[1] راجع في ذلك : د/ يوسف احمد النوافلة ، رسالة دكتوراه بعنوان "الإثبات الرقمي" ، مرجع سابق ، ص 28 ، ص 244 وما بعدها وراجع أيضا :

_ https://www.lexology.com/library/detail.aspx?g=29828d6d-8396-4070-9424-05ac2e0ecfae

[2] راجع في ذلك : د/ أحمد محمد عبدالرحمن، "نظرة حول نظام التقاضي الرقمي في مصر" ، مرجع سابق ، ص25 .

تزيد علي ثلاثين يوما قابلة للتجديد لمدة أو مدد آخري مماثلة[1] ،وهو ما يمكن الاستئناس به فى مجال القضاء المدنى .

خامسا :الإثبات بشهادة الشهود[2]

ترتب أدلة الإثبات علي درجات تأتي في أعلاها الإثبات الخطي أي بالكتابة وبعده مباشرة الإثبات الشفهي أي شهادة الشهود أو البينة، إلا إنه لا تقبل الشهادة للإثبات إلا في أحوال محددة نص عليها القانون .

ويقصد بشهادة الشهود قيام شخص من غير أطراف الخصومة بالإدلاء بأقواله أمام مجلس القضاء حول حقيقة وقائع تصلح محلا للإثبات نشأ عنها حق أو مركز قانوني لغيره[3].

وللمحكمة السلطة التقديرية بشأن الاستجابة لطلب الخصوم لسماع شهادة الشهود كدليل للإثبات من عدمه، فقد تري المحكمة أن المستندات والوثائق المكتوبة كافية للفصل في النزاع أو أن الواقعة التي سيتم الاستعانة بشأنها بالشهود قد أصبحت واضحة للمحكمة، كما قد تري أن الجوانب الموضوعية والقانونية للدعوي لم تكتمل وإنه يجب الاستعانة بشهادة الشهود من أجل أيضاح تلك الأمور، وللمحكمة أن تطلب من تلقاء نفسها سماع شهادة الشهود دون طلب من الخصوم وذلك إذا وجدت أن هناك فائدة جمة من سماعهم .

وقد أجاز قانون الإثبات المصري في حالة عدم استطاعة الشاهد الحضور إلي مقر المحكمة التي تنظر النزاع لأسباب جدية تمنعه من **ذلك كالمرض الشديد مثلا** ،ففي مثل هذه الحالة يمكن للمحكمة أن تندب أحد قضاتها للانتقال للشاهد وسماع أقواله وإثباتها في محضر تحقيق يوقعه القاضي المنتدب والكاتب .

---

[1] لدراسة أعمق في المسائل القانونية التي تعتمد علي التعامل مع الأدلة الرقمية وحماية الخصوصية ، انظر "القيود القانونية لحماية البيانات والخصوصية والشخصية في التعامل مع الأدلة الرقمية" ماريا فيرونيكا بيريز– Asinari المجلة الدولية للقانون الحاسبات و Technology ، Vol 18، No 2، 2004، pp 231–250.

[2] راجع في ذلك : د/ أحمد محمد عبدالرحمن، "نظرة حول نظام التقاضي الرقمي في مصر" ، مرجع سابق ، ص25 .

[3] راجع في ذلك : نظر Ken Chasse ، "السجلات التي تنتجها الكمبيوتر في إجراءات المحكمة" ، (1994) الملحق ياء لوقائع المؤتمر القانوني الموحد لكندا ، الاجتماع السنوي 1994 ، المحفوظ في :www.law.ualberta.ca/alri/ulc/94pro/ e94j.htm

كما أجازت المادة (90) من قانون الإثبات المصري بصفة استثنائية أن تكون الشهادة مكتوبة إذا كانت طبيعة الدعوي تسمح بذلك، ويجب أن يكون محرر الشهادة ممن تتوافر فيه الشروط العامة التي يجب أن تتوافر في الشاهد، أما فيما يخص شكل الشهادة فيجب أن تكتب الأقوال وتوقع وتؤرخ من الشاهد ويجب أن يتم توثيقها أمام مكتب التوثيق والشهر العقاري .

ويثور التساؤل في هذا الصدد في حالة تعذر حضور الشاهد لمقر المحكمة لظروف قهرية خارجة عن إرادته حول مشروعية استجواب الشهود في العالم الافتراضي عبر الإنترنت عن طريق استخدام تقنية الفيديوكونفرانس وذلك متي ثبت استحالة أو عدم ملائمة مثول الشاهد بنفسه أمام المحكمة، ومدي تأثير هذا الإجراء علي احترام مبدأ المواجهة وحق الدفاع عن طريق ضمان تقديم كل طرف لبيناته علي أكمل وجه؟

ويري البعض أن مناقشة الشهود وإن جاز إجراؤها في ظل التقدم التكنولوجي بطريقة رقمية عبر شبكة الإنترنت أو ما شابه[1] من وسائل الاتصالات اللاسلكية إلا أن مناقشة الشهود بالطريقة التقليدية هي الطريقة الأكثر قوة ووضوحا في استجلاء وجه الحقيقة نظرا لإمكانية مشاهدة تعبيرات وجه الشاهد ودرجة تأثره ومدي اتزانه وغيرها من العوامل التي قد تؤثر علي تقدير صحة الشهادة علي الواقعة محل الخلاف.

إلا أننا نري إنه في حالة تعذر حضور الشاهد لمقر المحكمة لسفره للخارج أو لمرضه الشديد أو إقامته بالمنزل أو المستشفى أو لوجود كوارث طبيعية كفيضان وغيره يستحيل معها مثول الشاهد بنفسه أمام المحكمة فإن إجراء استجواب الشهود عبر الإنترنت عن طريق استخدام تقنية الفيديوكونفرانس أو أي وسيط رقمي آخر سيتم استحداثه[2] .

---

[1] راجع في ذلك : د/ يوسف احمد النوافلة ، "الإثبات الرقمي" ، رسالة دكتوراه ، مرجع سابق ، ص 247 وما بعدها ، وراجع أيضا : طارق بن عبد الله بن صالح العمر ، أحكام التقاضي الرقمي ، رسالة دكتوراه ، ص299.

[2] راجع في ذلك :

Helmut Rümann، Electronic Documents. Security and Authenticity، Electronic Technology and Civil Procedure– New Paths to Justice from Around the World، Springer، 2012، p.235.

أما في حالة ما إذا كان الشاهد مقيما بالخارج فإن كان مصريا فإنه يمكن استدعائه عن طريق السفارة المصرية بالدولة التي يقيم بها ويحضر في موعد الجلسة المحدد لمقر السفارة المصرية ويتم الاتصال بالسفارة من قبل المحكمة أثناء انعقاد الجلسة عبر تقنية الفيديو كونفرانس وسماع شهادة الشاهد بمقر السفارة المصرية وكذلك الحال بالنسبة لغير المصريين بعد أن تتم مخاطبة البعثة الدبلوماسية للبلد التابع لها وأخذ موافقتها علي سماع شهادته بمقر السفارة المصرية بالخارج .

ومن ثم فإن سماع شهادة الشهود عن بعد عبر تقنية الفيديوكونفرانس هو وسيلة احتياطيه يمكن اللجوء إليها في حالة الضرورة بعد تعذر اللجوء إلي استدعاء الشخص المطلوب سماع شهادته أو تعذر إرسال إنابة قضائية للسلطة القضائية إلي موطن الشخص المطلوب سماع شهادته فعند استنفاد هاتين الوسيلتين وعدم إمكانية استخدامهما فإنه يجوز للسلطات القضائية أن تطلب القيام بهذا الإجراء عبر تقنية الفيديوكونفرانس أو أي وسيط رقمي آخر يتم استحداثه في هذا الأمر[1].

[1] راجع في ذلك : (تاريخ الدخول :2021/2/13)

_ https://www.tandfonline.com/doi/full/10.1080/15567280701418049?src=recsys

المطلب الرابع

تحديات قبول الأدلة الرقمية

تواجه الأدلة الرقمية التحدي ، في أنها تقنية فبعض القوانين لا تعترف بالأدلة التي تم الحصول عليها من خلال هذه المعاملة ، وتعامل كدليل ثانوي بسبب طبيعتها. ومن الأمثلة علي ذلك القسم 4 من قانون العقود (تنزانيا) .[1] **والتحديات الرئيسية** [2]التي ستواجه قبول الأدلة الرقمية (عبر الإنترنت) في طبيعتها في مجال المصادقة لوجود العديد من الفيروسات علي شبكة الإنترنت والتي من الممكن أن تصيب الملفات بالإضافة إلي الهاكر وهو ما سيكون معه من الصعب علي محكمة القانون أن تتأكد من عدم وصول أي متسللين إلي المعلومات أو التأكد من عدم إصابة الملفات التي يتم الحصول عليها رقميًا.

- **هل الأدلة الرقمية مقبولة؟**[3]

تقضي المحاكم أحيانًا بعدم قبول الأدلة الرقمية[4] نظرًا لأنه قد تم الحصول عليها دون إذن من الشخص المعني. ففي العديد من النظم القضائية ، تعتبر أوامر القبض ضرورية لأخذ أي أجهزة رقمية والتحقيق فيها ، وقد يؤدي ذلك إلي ظهور مشكلات ، خاصة في الحالات التي يتم فيها تحديد أدلة علي وجود جريمة أثناء التحقيق في جريمة أخري.

---

[1] راجع في ذلك : (تاريخ الدخول :2021/2/13)

_ https://www.lawteacher.net/free-law-essays/international-law/can-electronic-documents-be-used-as-evidence-international-law-essay.

[2] راجع في ذلك : (تاريخ الدخول :2021/2/13)

_ https://blog.signaturit.com/en/electronic-evidence-and-its-admissibility-in-court

[3] راجع في ذالك : (تاريخ الدخول :2021/2/13)

_ https://www.mailxaminer.com/blog/admissibility-of-electronic-evidence-in-court

[4] راجع في ذلك : (تاريخ الدخول :2021/2/13)

_ https://www.unodc.org/e4j/en/cybercrime/module-6/key-issues/digital-evidence-admissibility.html

- **آليات قبول الأدلة الرقمية في المحكمة:**

يستخدم واحد وتسعون بالمائة من البالغين علي الإنترنت اليوم شكلاً من أشكال الاتصال الرقمي بشكل منتظم في حياتهم اليومية. وبالتالي ، أصبحت الأدلة الرقمية جزءًا كبيرًا من العديد من القضايا المدنية والجنائية ؛ ومع ذلك ، هناك معايير محددة لتحديد قبول الأدلة الرقمية .

تم تدوين قواعد الإثبات الفيدراليةFRE)) ، وكذلك القواعد الفيدرالية للإجراءات المدنية (FRCP) ، بقصد توجيه المحاكم – المدنية والجنائية – لآلية قبول الأدلة. في حين تم تطوير FRCP و FRE لإملاء الإجراءات في المحاكم الفيدرالية ، حيث اعتمدت العديد من محاكم الولايات قواعد تعكسها عن قرب. كما أن قانون السوابق القضائية ، وكذلك الآراء الصادرة عن المحاكم ، توجه الأطراف في تحديد قبول الأدلة.

- **الأدلة الرقمية والقانون:**

في المملكة المتحدة ، تم استخدام قانون PACE لعام 1984 لتأسيس وتقييم الأدلة في المحكمة ولكن هذا القانون ينطبق علي إنجلترا وويلز وليس إسكتلندا. تم تطبيق CMA لعام 1990 (بصيغته المعدلة بموجب قانون الشرطة والعدل لعام 2006) عند ظهور قضايا جرائم الكمبيوتر في محاكم المملكة المتحدة . **و** يتبع الفاحصون عادةً المبادئ[1] التوجيهية التي تصدرها رابطة كبار ضباط الشرطة (ACPO) لتوثيق الأدلة وسلامتها[2]. تم تحديثها إلي الإصدار 5 في أكتوبر 2011 عندما تم استبدال الأدلة المستندة إلي الكمبيوتر بالأدلة الرقمية التي تعكس تطور التحقيق في حوادث أمن المعلومات في سياق أوسع. وهذه المبادئ هي :

<u>المبدأ</u> 1: يجب ألا يغير أي إجراء تتخذه وكالات إنفاذ القانون ، الأشخاص العاملون في تلك الوكالات أو وكلائهم ، البيانات التي يمكن الاعتماد عليها لاحقًا في المحكمة.

---

[1] راجع في ذلك : (تاريخ الدخول :2021/2/13)

– https://en.wikipedia.org/wiki/Digital_evidence Tech. 5 (2011)

[2] راجع في ذلك : (تاريخ الدخول :2021/2/13)

– https://www.bcs.org/content-hub/presenting-digital-evidence-to-court

المبدأ 2: في الحالات التي يجد فيها الشخص أنه من الضروري الوصول إلي البيانات الأصلية ، يجب أن يكون ذلك الشخص مختصًا بالقيام بذلك ويكون قادرًا علي تقديم أدلة تشرح أهمية أفعالهم والآثار المترتبة عليها.

المبدأ 3: يجب إنشاء والحفاظ علي سجل لجميع العمليات المطبقة علي الأدلة الرقمية.

المبدأ 4: يتحمل الشخص المسؤول عن التحقيق المسؤولية الكاملة عن ضمان التقيد بالقانون وهذه المبادئ.

يتم قبول هذه المبادئ التوجيهية علي نطاق واسع في محاكم إنجلترا وإسكتلندا ، لكنها لا تشكل شرطًا قانونيًا وإنما استخدامها طوعي .

- **القواعد الفيدرالية لقبول الأدلة الرقمية[1] :**

طبقت العديد من المحاكم في الولايات المتحدة قواعد الإثبات الفيدرالية علي الأدلة الرقمية بطريقة مماثلة للوثائق التقليدية[2] ، علي الرغم من وجود اختلافات مهمة مثل عدم وجود معايير وإجراءات ثابتة. بالإضافة إلي ذلك ، تميل الأدلة الرقمية إلي أن تكون أكثر ضخامة ، وأكثر صعوبة في التدمير ، وتعديلها بسهولة ، وتكرارها بسهولة ، وربما تكون أكثر تعبيرية ، ومتاحة بسهولة أكبر ، وفي ديسمبر 2006 ، تم سن قواعد جديدة صارمة داخل القواعد الفيدرالية للإجراءات المدنية التي تتطلب الحفاظ علي الأدلة المخزنة رقميًا والكشف عنها. فغالبًا ما تتعرض الأدلة الرقمية للهجوم بسبب أصالتها نظرًا للسهولة التي يمكن بها تعديلها .

تستخدم العديد من التطبيقات والمواقع الرقمية والأجهزة الرقمية خدمات التخزين السحابية. المستخدمين وبالتالي ، يمكن تخزين البيانات كلياً أو علي شكل أجزاء بواسطة العديد من مقدمي الخدمات المختلفين في خوادم في مواقع متعددة ولهذا السبب ، يعد استرداد البيانات من

---

[1] راجع في ذلك : (تاريخ الدخول :2021/2/13)

– ISO / IEC 27037 ؛ Cybercrime Module 4 on Introduction to Digital Forensics

[2] للوقوف علي مقبولية الأدلة الرقمية في المحكمة : (تاريخ الدخول :2021/2/13)

— https://www.tandfonline.com/doi/full/10.1080/15567280701418049?src=recsys

هؤلاء أمرًا صعبًا[1]. وتختلف إجراءات التجميع تبعًا لنوع الجهاز الرقمي والموارد العامة والخاصة حيث توجد الأدلة الرقمية (علي سبيل المثال ، أجهزة الكمبيوتر والهواتف والوسائط الرقمية والسحابة الرقمية ؛ لكل منها طريقة للمعالجة في **الطب الشرعي الرقمي**[2] وخاصة فيما يتعلق بالوسائط المتعددة والفيديو والجوال .[3]

تقوم العديد من **محاكم الولايات المتحدة** الآن بتطبيق قواعد الإثبات الفيدرالية علي الأدلة في شكل رقمي بطريقة مشابهة تمامًا للطريقة التي يتم بها تطبيقها علي الأعمال الورقية

---

[1] لمزيد من المعلومات ، انظر موقع : Cybercrime Module 7 حول التعاون الدولي ضد الجريمة السيبرانية وقد آثرنا الإشارة دون الإفاضة لعدم اتساع المجال لذالك .

[2] أدي التطور السريع للتكنولوجيا واستخدام الأجهزة الرقمية مثل الهواتف المحمولة وأجهزة الكمبيوتر والأجهزة اللوحية ، والتي أصبحت جزءًا لا غني عنه في المجتمع الحديث ، إلي انتقال كبير من إنشاء البيانات المادية إلي البيانات الرقمية.

ونتيجة لذلك ، أصبح دور الطب الشرعي الرقمي في مكافحة الجريمة أكثر أهمية ، ومن الأهمية بمكان أن تقوم شركات القانون والمحاكم بوضع استراتيجية مدروسة لمثل هذه التحقيقات. فيPender hill ، أوضحت المحكمة العليا أن المحاكم يجب أن تستجيب بشكل مناسب للتغيرات التقنية التي تحدث. فالأدلة مقبولة قانونيا عندما: تقدم لإثبات وقائع القضية ؛ و لا ينتهك الدستور أو القوانين القانونية الأخرى. وراجع في ذلك أيضا : (تاريخ الدخول :2021/2/13)

- https://www.lexology.com/library/detail.aspx?g=29828d6d-8396-4070-9424-05ac2e0ecfae
- https://www.researchgate.net/publication/327644306_Digital_Forensics_Review_of_Issues_in_Scientific_Validation_of_Digital_Evidence
- https://economictimes.indiatimes.com/news/politics-and-nation/courts-can-rely-on-electronic-records-without-certificate-supreme-court/articleshow/62777759.cms
- http://www.jurisdiction.com/ecom4.htm

[3] راجع في ذلك : (تاريخ الدخول :2021/2/13)

- https://www.unodc.org/e4j/en/cybercrime/module-6/key-issues/handling-of-digital-evidence.html

التقليدية ، ومع ذلك تم الاعتراف بالاختلافات من حيث الإجراءات والمعايير المعمول بها. الأدلة الرقمية هي أيضًا أكثر ضخامة ويصعب تدميرها فضلاً عن تكرارها أو تعديلها بسهولة أكبر. أدخلت القواعد الفيدرالية للإجراءات المدنية قواعد جديدة تتطلب الكشف عن جميع الأدلة المخزنة رقميًا وحفظها. علي الرغم من أن الأدلة الرقمية تتعرض للهجوم بشكل متكرر بسبب وجود مشاكل محتملة في أصالتها ،[1]إلا أن المحاكم بدأت الآن في رفض هذه الحجج ما لم يكن هناك دليل علي أنه تم التلاعب بالأدلة.

وفي المملكة المتحدة ، أصبحت سجلات أجهزة الكمبيوتر التي تُسمع بالسمع مقبولة في عام 1995 من خلال تعديل قانون الأدلة المدنية لعام 1968 بسبب عدم وجود اعتراضات من جانب أطراف علي هذه الأدلة علي مدار فترة زمنية ، مما يشير إلي قبولها بين عامة الجمهور.

و في الهند ، جاء التغيير في المواقف مع تعديل قانون الأدلة الهندي في عام 2000. تم إدخال القسمين A و B في الفصل المتعلق بالأدلة الوثائقية. ينص القسم A علي أنه يجوز قبول محتويات السجلات الرقمية كدليل إذا تم الامتثال للمعايير المنصوص عليها في القسم .B تنص المادة B علي أنه يجب اعتبار المستندات ، مما يجعلها دليلًا أساسيًا ، إذا كان الكمبيوتر الذي أنتج السجل قيد الاستخدام بانتظام ، فالمعلومات التي يتم إدخالها في الكمبيوتر كانت جزءًا من الاستخدام المنتظم للكمبيوتر وكان الكمبيوتر يحتوي علي سجل كان يعمل بشكل صحيح . وينص كذلك علي أن جميع مخرجات الكمبيوتر تعتبر منتجة بواسطة الكمبيوتر نفسه ، سواء تم إنتاجه بشكل مباشر أو غير مباشر ، سواء بتدخل بشري أو بدونه. يلغي هذا البند مفهوم الأدلة الحاسوبية علي أنه سماع.

---

[1] وللوقوف علي المقبولية القانونية للأدلة الرقمية راجع في ذلك :

– https://www.tandfonline.com/doi/abs/10.1080/13600860420002235 08?src=recsys&journalCode=cirl20(8/1/2021 : تاريخ آخر دخول علي الموقع)

المطلب الخامس

موقف النظم القضائية المقارنة

يمكن القول بداية [1] أن نظم الإثبات في القانون المقارن قد انقسمت إلي مدرستين أساسيتين الأولي تتبع نظام الإثبات المعنوي أو المطلق والذي فيه لا يقيد المشرع أطرف الرابطة الإجرائية بتقديم أدلة معينة بل للقاضي أن يقتنع بأي دليل وهذا هو النظام السائد في القانون الفرنسي ومن يسير علي نفس نهجه من التشريعات.

أما المدرسة الثانية فتتبع نظام الإثبات القانوني أو المقيد والذي فيه يحدد القانون الأدلة التي يجوز تحقيقها والاستناد إليها في الحكم وهذا هو النظام السائد في القانون الإنجليزي ومن يسير علي نفس نهجه من التشريعات.

وعلي الرغم من اختلاف نظام المدرستين في الإثبات إلا أن هناك ضوابط معينة تحكم الأدلة الناتجة عن الحاسب الآلي بشكل عام يلتزم بها القضاء لتجنب سوء التصرف ولدعم وحماية حقوق الأطراف أو غيرها من الحقوق محل الاحترام وهذه الضوابط مدارها أصل البراءة و ما يتفرع عنه من نتائج وآثار وما يستتبعه من وجوب توافر شروط معينة في المخرجات الرقمية [2]يتأكد بها القاضي أولا من أن الدليل الرقمي لم يتم التلاعب فيه[3] حتي يمكنه الحكم بالبراءة أو بالإدانة .

كما يجب أن تكون عقيدة القاضي و اقتناعه بالإدانة قد استمدت من دليل رقمي طرح بالجلسة لأن القاعدة هي إنه " لا يحكم إلا بناء علي التحقيقات التي تحصل بالطرق والشروط القانونية " و ليس بناء علي معلوماته الشخصية أو علي ما قد يكون قد رآه بنفسه أو حقيقة في غير مجلس القضاء كما ينبغي ألا يؤسس القاضي حكمه علي دليل ناتج عن أي وسيط رقمي لحقه سبب يبطله ويعدم أثره عليه و تحقيقا لليقينية والشفوية والمشروعية في الدليل فان مجمل شروط قبول المخرجات الرقمية تتلخص في المبادئ الثلاثة التالية:

---

[1] راجع في ذلك : د/ راشد بن حمد البلوشي ، حجية المخرجات الرقمية في الإثبات " ، ص 19 وما بعدها.

2 راجع في ذلك: د/عبد التواب مبارك ، الدليل الرقمي أمام القاضي المدني ، دار النهضة العربية، مرجع سابق ، ص 57 :107.

[3] راجع في ذلك: د/عبد التواب مبارك ، الدليل الرقمي أمام القاضي المدني ، مرجع سابق ، ص 110 :173

1- مبدأ يقينيه المخرجات الرقمية.

2- مبدأ وجوب مناقشة المخرجات الرقمية

3- مبدأ مشروعية المخرجات الرقمية.

- **مبدأ يقينية المخرجات الرقمية[1] :**

جـرت عـدة محـاولات فـي الفقه تتعلق بتقسـيمات اليقين حيث فرق البعض بين يقين البديهيات أو المسلمات المقبولة عامة في الضـمير الإنسـاني والتي من أبرز الأمثلة عليها : اليقين الرياضـي وبين اليقين الاستقرائي وهو الذي يعقد علي الاستدلال بالقياس لإثبات شئ معين . كما فرق البعض الآخر بين اليقين الميتافيزيقي أو الغيبي وهو الذي يستنبط من أمور غيبية واليقين الفيزيقي أو الطبيعي وهو الذي يستنبط من إدراك الحواس البشرية واليقين المعنوي وهو الذي يستنبط من نشاط الآخرين غير أن الراجع في الفقه الإجرائي المعاصر هو تقسيم اليقين من حيث مصدره إلي يقين قانوني ويقين معنوي.

فاليقين القانوني يعني : تلك الحالة الناجمة عن القيمة التي يضفيها القانون علي الأدلة ويفرضـها علي القاضـي ، فهو نوع من اليقين يتلقاه القاضـي عن إرادة المشرع وهذا النوع من اليقين هو السائد في القانون الإنجليزي.

إلا إن القانون العام في إنجلترا[2] لم يعد يأخذ بنطريه الأدلة القانونية علي الإطلاق بل بدأ يتقبل مبدأ حرية تقدير الأدلة لذلك فقد أصبح الحديث عن الإدانة بدون أي شك معقول أو الإدانة الخالية من أي شك هو السائد في القانون الإنجليزي حالياً.

ومن هذا المنطلق نجد أن **القضاء الإنجليزي** يملك حرية الحكم بالإدانة بناء علي شهادة شخص واحد طالما أن هذه الشهادة تحقق اليقين حيث أن القاعدة العامة في إنجلترا هي أن المحكمة لا يجب أن تدين المدعي عليه إلا عندما تكون عناصر الجريمة قد تم إثباتها بعيداً عن كل شك معقول.

---

[1] راجع في ذلك : د/ راشد بن حمد البلوشي ،حجية المخرجات الرقمية في الإثبات، مرجع سابق ص 11 وما بعدها .

[2] راجع في ذلك : د/ راشد بن حمد البلوشي ، حجية المخرجات الرقمية في الإثبات ، مرجع سابق ص 12

وإذا انتقلنا لمناقشة يقينية المخرجات الرقمية نجد أن قانون البوليس والإثبات الجزائي في **بريطانيا** يشترط حتي تتحقق يقينية المخرجات الرقمية أن تكون البيانات دقيقة وناتجة عن حاسب يعمل بصورة سليمة.

اما في **فرنسا** فإنه لا محل لدحض أصل البراءة وافتراض عكسه إلا عندما يصل اقتناع القاضي إلي حد الجزم واليقين ، والأمر لا يختلف في ذلك بالنسبة لمخرجات الحاسب الآلي إذ يشترط القانون الفرنسي في المخرجات الرقمية أن تكون يقينية حتي يمكن الحكم بالإدانة ذلك إنه لا محل لدحض قرينة البراءة وافتراض عكسها إلا عندما يصل اقتناع القاضي إلي حد الجزم واليقين ويتم الوصول إلي ذلك عن طريق ما تستنتجه وسائل الإدراك المختلفة للقاضي من خلال ما يعرض عليه من مخرجات الحاسب الآلي سواء كانت مخرجات لا ورقية أو رقمية كالأشرطة المغناطيسية والأقراص المغناطيسية والمصغرات الفيلمية وغيرها من الأشكال الرقمية غير التقليدية للتكنولوجيا التي تتوافر عن طريق الوصول المباشر لهذه الأدلة أم كانت مجرد عرض لهذه المخرجات المعالجة رقمياً.

أما في **سلطنة عمان** فقد أكدت المحكمة العليا علي أصل البراءة وذلك في حكمها الصادر بالقرار رقم 50 في الطعن رقم 2004/22م في جلسة 2004/3/2م والذي جاء فيه أن " يكفي للقضاء بالبراءة مجرد التشكك المعقول في صحة إسناد التهمة إلي المتهم أو لعدم كفاية الأدلة لأن الأصل في الإنسان البراءة وأن الجريمة صورة من صور السلوك الشاذ الخارج عن المألوف فقد وجب الاحتياط في نسبتها علي شخص معين استصحاباً لهذه القاعدة الأصولية".[1]

وهكذا يستطيع القاضي من خلال ما يعرض عليه من مخرجات الحاسب الآلي وما ينطبع في ذهنه من تصورات واحتمالات بالنسبة لها أن يحدد قوتها الاستدلالية علي صدق نسبة الجريمة المعلوماتية إلي شخص معين من عدمه، فكأن القاضي يصل إلي يقينية المخرجات الرقمية عن طريق نوعين من المعرفة:

أولهما: المعرفة الحسية التي تدركها الحواس من خلال معاينة هذه المخرجات وتفحصها.

وثانيهما: المعرفة العقلية التي يقوم بها القاضي عن طريق التحليل والاستنتاج من خلال الربط بين هذه المخرجات والملابسات التي أحاطت بها و اذا لم ينته القاضي إلي الجزم بنسبه

[1] راجع في ذلك : د/ راشد بن حمد البلوشي ،حجية المخرجات الرقمية في الإثبات، ص13

الفعل او الجريمة المعلوماتية إلي المتهم المعلوماتي كان من المتعين عليه أن يقضي بالبراءة فالشك يجب أن يفسر لصالح المتهم.

- **مبدأ وجوب مناقشة المخرجات الرقمية[1] :**

الأصل الذي يحكم إجراءات المحاكمة هو أن تكون المرافعة شفوية وحضورية والمقصود بالمرافعة هنا جميع إجراءات التحقيق النهائي الذي تجريه المحكمة ومفهوم مبدأ وجوب مناقشة المخرجات الرقمية يعني بصفة عامة أن القاضي لا يمكن أن يؤسس اقتناعه إلا علي العناصر الإثباتية التي طرحت في جلسات المحاكمة وخضعت لحرية مناقشة أطراف الدعوي، ولا يختلف الأمر بالنسبة للمخرجات الرقمية بوصفها أدلة إثبات[2] إذ ينبغي أن تطرح في الجلسة وأن يتم مناقشتها في مواجهة الأطراف وتأسيساً علي ذلك يجب أن تبدي شفاهه ، وفي حضور جميع الخصوم ، كافة الطلبات والدفوع والمرافعات فتطرح الأدلة عليهم للمناقشة فيها ، سواء كانت أدلة تقليدية أو أدلة رقمية ، ويسمع شهود الدعوي من جديد في مواجهتهم والخبير يجب أن يحضر ويقرأ تقريره شفوياً في الجلسة كما أن متحصلات الجريمة التي تم ضبطها يجب أن تعرض علي القاضي شخصياً وذلك حتي يقيم اقتناعه علي ما شاهده وسمعه بنفسه في المحكمة، وتعد

---

[1] راجع في ذلك : د/ راشد بن حمد البلوشي ، حجية المخرجات الرقمية في الإثبات ، مرجع سابق ص 13 وما بعدها ، وراجع أيضا: د/ يوسف احمد النوافلة ، "الإثبات الرقمي" ، رسالة دكتوراه ، مرجع سابق ، ص 232 وما بعدها .

[2] راجع في ذلك :

- https://www.unodc.org/e4j/en/cybercrime/module-6/key-issues/handling-of-digital-evidence.html
- https://www.tandfonline.com/doi/full/10.1080/15567280500541462?src=recsys
- https://www.lawteacher.net/free-law-essays/international-law/can-electronic-documents-be-used-as-evidence-international-law-essay.php
- https://blog.signaturit.com/en/electronic-evidence-and-its-admissibility-in-court

الشفوية والحضورية من الركائز الأساسية التي يترتب علي إغفالها بطلان إجراءات المحاكمة لما في هذا الإغفال من إهدار لحق الدفاع بحرمانه من الإلمام بالأدلة المقدمة ضده لتفنيدها.

وهذا ما أكدت عليه المحكمة العليا في سلطنة عمان في حكمها الصادر بالقرار رقم 83 في الطعن رقم 51/2004م- جلسة 13/4/2004م والذي جاء فيه أن (كل دليل تعتمد عليه المحكمة في حكمها يجب أن يكون قد طرح شفوياً في الجلسة وجرت في شانه المناقشة الشفوية كذلك ويستمد القاضي اقتناعه من حصيلة هذه المناقشات الشفوية ولا يستمده من المحاضر المكتوبة).

وبناءا علي ذلك فإن كل دليل رقمي يجب أن يعرض في الجلسة ليس من خلال ملف الدعوي أو التحقيق الابتدائي لكن بصفة مباشرة أمام القاضي ، وهذه الأحكام تنطبق علي كافة الأدلة المتولدة عن الحاسبات الآلية[1] ، وأيضا بالنسبة لشهود الجرائم المعلوماتية الذين يكون قد سبق أن سمعت شهادتهم في التحقيق الابتدائي فإنه يجب أن يعيدوا أقوالهم مرة آخري من جديد

[1] نصت المادة 1/10 من القانون النموذجي للتجارة الرقمية علي أن: (عندما يقضي القانون الاحتفاظ بمستندات أو سجلات أو معلومات بعينها، يتحقق الوفاء بهذا المقتضي إذا تم الاحتفاظ برسائل البيانات، شريطة مراعاة الشروط التالية:

أ-تيسر الاطلاع علي المعلومات الواردة فيها علي نحو يتيح استخدامها في الرجوع إليها لاحقاً.

ب-الاحتفاظ برسالة البيانات بالشكل الذي أنشئت أو أرسلت أو استلمت به أو بشكل يمكن إثبات أنه يمثل بدقة المعلومات التي أنشئت أو أرسلت أو استلمت.

ج-الاحتفاظ بالمعلومات-إن وجدت – التي تمكن من استبانة منشأ رسالة البيانات وجهة وصولها وتاريخ ووقت إرسالها واستلامها(

وهو ما نصت علية المواد 8/1 من قانون إمارة دبي، و8/أ من القانون الأردني، ولفصل الرابع من القانون التونسي وأغلب القوانين العربية ، راجع في ذلك : د. هشام عبد السيد الصافي ، القضاء الإداري المصري والتكنولوجيا الحديثة ، مقال نشر في مجلة جيل الأبحاث القانونية المعمقة ،العدد 17 ، ص 49 وما بعدها

أمام المحكمة[1] ، كذلك فإن خبراء الأنظمة المعلوماتية علي اختلاف تخصصاتهم ينبغي أن يمثلوا أمام المحاكم لمناقشتهم أو مناقشة تقاريرهم التي خلصوا إليها إظهاراً للحقيقة وكشفاً للحق .

وهذا يعني أن المخرجات الرقمية سواء كانت مطبوعة أم بيانات معروضة علي شاشة الكمبيوتر[2] أم كانت بيانات مدرجة في أسطوانات مضغوطة CD /DVD فإنه يجب مناقشتها وتحليلها[3].

ولا يجوز أن يحيل الحكم في شأن وقائع الدعوي ومستنداتها إلي دعوي آخري غير مطروحة ، وهذا ما أكدت عليه المحكمة العليا في سلطنة عمان في حكمها الصادر بجلسة 29/10/2002م- الطعن رقم 72/2002م حيث جاء في حكمها" أن تقدير الدليل بالصورة التي تكشف قناعة المحكمة من إطلاقات محكمة الموضوع لا تجوز إثارته أمام المحكمة العليا."

---

[1] راجع في ذلك : د/ يوسف احمد النوافلة ، "الإثبات الرقمي" ، رسالة دكتوراه ، مرجع سابق ، ص 232 وما بعدها ، وراجع أيضا :

- https://www.bcs.org/content-hub/presenting-digital-evidence-to-court/

[2] راجع في ذلك :

Valérie Sédallian: L´archivage de l´acte électronique, juriscom.net,8 juillet 2002, le sur sit: http://www.juriscom.net..

وما يؤكد ذلك ما نصت عليه المادة 1316/1 من القانون المدني الفرنسي علي أن (تتمتع الكتابة الرقمية بالحجية في الإثبات شأنها في ذلك شأن الكتابة علي دعامة ورقية بشرط.... أن تعد وتحفظ في ظروف من طبيعتها ضمان سلامتها"، وقد أضاف المشرع الفرنسي فقرة جديدة للمادة 1317 من القانون المدني)..... ويمكن أن يكتب علي دعامة رقمية علي أن تعد وتحفظ طبقا للضوابط التي يحددها مجلس الدولة)، راجع نصها بالفرنسية:

“ART1317-2du code ” peut être dressé sur support électronique s’il est établi et conservé dans des conditions fixées par en Conseil d’ Etat.”

[3]: راجع في ذلك

- https://www.lawteacher.net/free-law-essays/international-law/can-electronic-documents-be-used-as-evidence-international-law-essay.php
- https://blog.signaturit.com/en/electronic-evidence-and-its-admissibility-in-court

أو أن تعتمد المحكمة علي أدلة ووقائع استقتها من أوراق قضية آخري لم تكن مضمومة للدعوي التي تنظرها للفصل فيها ولا مطروحة علي بساط البحث بالجلسة تحت نظر الخصوم لكن يلاحظ إنه وإن كان يجب أن يصدر الحكم عن عقيدة للقاضي يستقيها هو مما يجريه من التحقيقات مستقلاً في تحصيل هذه العقيدة بنفسه لا يشاركه فيها غيره إلا إن ذلك لا يعني حرمان القاضي بصفة مطلقة من الأخذ برأي الخبير متي اقتنع به هو حيث يتعين عليه في هذه الحالة أن يبين أسباب اقتناعه بهذا الرأي باعتباره من الأدلة المقدمة إليه في الدعوي المطلوب منه أن يفصل فيه.

- **مبدأ مشروعية المخرجات الرقمية[1] :**

كل الأدلة التي يتم الحصول عليها عن طريق انتهاك حق أساسي للمتهم تكون باطلة ولا يمكن التمسك بها ومراعاتها في أي مرحلة من مراحل الإجراءات ومن ثم فإنه يجب أن تكون المخرجات الرقمية أو الأدلة الناتجة عن الحاسب الآلي صحيحة ومشروعة حتي يمكن الحكم بالإدانة.

أ .اختبار الإعلان الرقمي للكتابة:

أظهر المشرع الفرنسي الحق في أن يأخذ في الاعتبار التطورات التقنية لمجتمع المعلومات من خلال إنشاء القانون عدد 2000–230 المؤرخ 13 مارس 2000 " لتكييف قانون الإثبات لتكنولوجيا المعلومات. حيث تنص المادة 1316–1 من القانون المدني علي أن " الكتابة الرقمية تقبل كدليل بنفس الطريقة التي تكتب بها الكتابة في شكل ورقي، شريطة أن يكون الشخص الذي تكتب كتاباته ممكنا ، وأن يتم إنشاؤها والحفاظ عليها في ظروف من شانها أن تضمن سلامتها . وبالتالي لم يعد هناك أي تضارب بين الأدلة الورقية والأدلة الرقمية (المادة 1316–2 من القانون المدني).

[1] راجع في ذلك : د/ راشد بن حمد البلوشي ، حجية المخرجات الرقمية في الإثبات ، مرجع سابق ص 16 وما بعدها ، وراجع أيضا: د/ يوسف احمد النوافلة ، "الإثبات الرقمي" ، مرجع سابق ، ص 175 وما بعدها .

وتعطي المادة 1316-3 و 1316-4 من القانون المدني، علاوة علي ذلك، تعريفا للقوة الإثباتية للكتابة في شكل رقمي، معترفة بأن هذه القوة تخضع لشروط معينة: فمن ناحية، يجب ضمانه، ومن ناحية آخري، يجب إنشاء المساءلة أمام مقدم البلاغ.

ولذلك فإن التوقيع الرقمي له نفس القيمة القانونية للتوقيع المكتوب بخط اليد، شريطة أن تكون العملية موثوق بها، وترد الشروط التي تسمح بالاستفادة من هذا الافتراض القانوني للموثوقية بالتوقيع الرقمي في المرسوم عدد 272 لسنة 2001 المؤرخ 30 مارس 2001.

ومن ناحية آخري، يكرس القانون المؤرخ 13 آذار / مارس 2000 إمكانية قيام الموظفين العموميين بوضع الوثائق الأصلية وإبقائها في شكل رقمي وهذه النقطة الأخيرة هي ثورة قانونية حقيقية مما يثير الحذر الشديد في تطبيقه .

ويحدد المرسوم المذكور أعلاه المؤرخ 30 آذار / مارس 2001 والمتعلق بتطبيق المادة 1316-4 من القانون المدني والمتعلق بالتوقيع الرقمي الشروط الواجب توافرها للاستفادة من افتراض موثوقية عملية التوقيع الرقمي.بحيث يجب أن يكون التوقيع الرقمي آمن ويضمن الخصوصية ولذلك، فمن الضروري إنشاء أجهزة التحقق من صحة التوقيع الرقمي والتي سيتم تنفيذها من خلال استخدام الشهادات الرقمية المؤهلة لضمان سلامة هذا التوقيع ولذلك، يبدو أن هذا القانون يحقق مزايا جدية من حيث توفير الوقت للإجراءات كما يجب إنشاء آليات لإضفاء الطابع المادي علي المرافعات من أجل حماية أمن التبادلات القانونية " إجراءات حماية مستندات الدعوي المقامة رقميا إجراءات حماية مستندات الدعوي المقامة رقميا والتي تهدف إلي تفادي تعديل أو تغيير أو تدمير ملفاتها سواء تم ذلك عمدا أو بإهمال[1] .

وبالتالي، فإن اعتماد هذه القوانين في 13 آذار / مارس 2000، دليل علي المنافسة غير الملموسة في المستقبل بين الأدلة الورقية والاقتناع بأن استخدام التكنولوجيات الجديدة أمر منطقي للإجراءات المدنية.

[1] راجع في ذلك : نص المادة 13 من قانون تعديل بعض أحكام قانون المحاكم الاقتصادية رقم 120 لسنة 2008 .

ولا تزال الحجج المؤيدة لإدخال تكنولوجيات جديدة للإجراء المدني تستند إلي النقطة التي حظيت بتقدير إيجابي من جانب المشرعين الذين يحاولون تدريجيا تحديث النظام القضائي الفرنسي بالاستناد إلي هذه الأدوات وتتمتع هذه الأخيرة أيضا بميزة تكييفها مع المتطلبات الأوروبية التي تحكم المؤسسات القضائية.

- **نطاق قبول الأدلة الرقمية.**[1]

وباعتماد القانون المؤرخ 13 آذار / مارس 2000، كان طموح المشرع الفرنسي هو تكييف القواعد الحالية لقانون الإثبات مع الواقع ، في إشارة إلي أن الكتابة الرقمية لها نفس القيمة الإثباتية للكتابة الورقية علي النحو التالي:

أ- القوة الإثباتية للكتابة الرقمية عن طريق التصديق:

بيد أن الهدف الرئيسي من القانون المؤرخ 13 آذار / مارس 2000 هو تحويل الأدلة الحاسوبية إلي أدلة من الدرجة الأولي عن طريق الاعتراف بأن الكتابة الرقمية تقبل كأدلة كما هي في شكل ورقي .وبالتالي، فإن التصديق، والآلية القانونية لإضفاء الطابع المادي علي الدليل يزيد من قوة الدليل الرقمي.

والواقع أن الضمانات الورقية معروفة: النزاهة والمتانة وإمكانية التوقيع ، وهو نفس ما يعطيه التصديق للدليل الرقمي.

وأخيرا، يبدو أن استخدام شهادة الطرف الثالث " **التصديق**[2] " يزيد من تقليل مخاطر الاحتيال .في الواقع.

---

[1] راجع في ذلك : د/ يوسف احمد النوافلة ، رسالة دكتوراه بعنوان "الإثبات الرقمي" ، مرجع سابق ، ص 175 وما بعدها.

[2] راجع في ذلك : المستشار د/ ياسر أحمد بدر ، الاتجاهات الحديثة في التصديق الرقمي ، بحث مقدم للمؤتمر العلمي السنوي الحادي عشر ، كلية الحقوق ، جامعة أسيوط ، بعنوان الاتجاهات الحديثة في القانون الإجرائي ، في الفترة من 29 :30/ 2017/3 ، ص4 وما بعدها .

ومن الناحية العملية، يحل التصديق[1] المخاوف المشروعة من مصادقة المؤلف وسلامة المحتوي من خلال اقتراح إزالة الطابع المادي لوثائق الإجراءات الأمنة والقانونية .

ب- إدارة نزاع الإثبات:

والغرض من الصراع بين الطرق التقليدية للإثبات هو في الواقع ضمان أولوية الكلمة المكتوبة .ومع ذلك، بما أن نوعين من الكتابات معترف بهما علي إنهما لهما نفس القيمة الإثباتية، فإن التعايش بين هاتين الوسيلتين الإثباتيتين ما زال يتعين تسويته[2] .

[1] راجع في ذلك : د/ أشرف جابر سيد ، الوجيز في أصول الإثبات ، دار النهضة العربية ، 2004 ، ص97

الخاتمة والنتائج

هذا وبعد ان عرضنا بالمبحث الأول للاكتشاف الإلكترونى من حيث ماهيته الاكتشاف الإلكترونى وكيفية الإدارة الذكية للمعلومات ، ومتطلبات الاكتشاف الإلكترونى ، و تحديات الاكتشاف الإلكترونى ،والتخطيط الناجح للاكتشاف الإلكترونى ،والذكاء الاصطناعي والاكتشاف الإلكترونى ; كما عرضنا بالمبحث الثانى لـلأدلة الرقمية من حيث ماهيتها ،ومتطلبات الإثبات بالأدلة الرقمية ،وأنواع الادلة الرقمية ،و تحديات قبول الأدلة الرقمية الأدلة الرقمية ثم ختمنا بـموقف النظم القضائية المقارنة يتضح الآتى:

- يتيح الجمع بين التعرف على الأنماط البشرية الطبيعية ودعم قدرات التعلم الذاتي للذكاء الاصطناعي للمحامين القدرة على استخراج المعلومات ذات الصلة بشكل أسرع وأسهل من أي وقت مضى.
- للحفاظ على المعرفة والمهارة المطلوبة ، يجب على القانونيين مواكبة التغييرات في القانون وممارساته ، بما في ذلك الفوائد والمخاطر المرتبطة بالتكنولوجيا ذات الصلة ، الانخراط في الدراسة والتعليم المستمر والامتثال لجميع متطلبات التعليم القانوني المستمر.
- يعد اعتماد تقنية الذكاء الاصطناعي حاليًا وسيلة لاكتساب العديد من المزايا، و مع تطور التكنولوجيا قد لا يمر وقت طويل قبل أن تصبح التزامًا أخلاقيًا كأداة ليس هناك سبب وجيه لعدم استخدامها.
- ستكون هناك عولمة للخصوصية، تكون فيها مبادئ ممارسة المعلومات متسقة نسبيا في جميع أنحاء العالم، مع زيادة المساءلة وتشديد جهود الإنفاذ .
- توقع نشوء اقتصاد من المعلومات المفتوحة التي تتغلغل عبر الحدود الجغرافية، حيث يطلع على البيانات أعداد متزايدة من الأشخاص، ومن ثم سيكون من الضروري زيادة الشفافية وتحسين توعية مستهلكي البيانات على مستوى العالم.
- برغم أن الدول التي تمتلك تشريعات تحفظ خصوصية مواطنيها من تعرض بياناتهم الشخصية للسرقة أو التجسس أو استغلالها في الأغراض التجارية والدعائية، إلا أن هذه

التشريعات غير واضحة كما أنها بها العديد من الثغرات القانونية كونها اعتمدت على معايير قديمة ولم تغطي جميع حالات التي تعترض الخصوصية الرقمية.

- إن أهم ما قد يحافظ على خصوصية الأفرد الرقمية ليس فقط تشريع قانوناً ولكن أيضا ضمان تطبيقه بالإضافة لقابليته للتعديل بناء على ما قد يجد من انتهاكات تمس الخصوصية الرقمية.
- لوحظ أنه مع تزايد تأثير التكنولوجيا في الحياة اليومية ، أصبح تقديم الأدلة الإلكترونية ضرورة في معظم الحالات لإثبات إدانة المتهم أو مسؤولية المدعى عليه . وهو ما أدى لتحول في العقلية القضائية خلال العشرين عامًا الماضية وبناءا عليه عدلت معظم النظم القانونية في جميع أنحاء العالم قوانينها لاستيعاب هذا التغيير.
- تتزايد احتمالات التلاعب بالأدلة الإلكترونية ، لذا يجب على المحكمة اتخاذ جميع الاحتياطات الممكنة ضد التعديلات المحتملة . فالمطبوعات البسيطة لرسائل البريد الإلكتروني أو الرسائل الفورية أو التعليقات على وسائل التواصل الاجتماعي هي مجرد نسخ يمكن استبعادها من مصطلح دليل إلكتروني ، بدون طعن عليها ، إذا لم تكن هناك وسائل أخرى للتحقق من صحتها.
- من الضروري اللجوء إلى خبير ، أو وجود شهادة تعزز البريد الإلكتروني كوسيلة للإثبات ، أو مزود خدمة موثوق به يضمن التحقق من التوقيع إلكتروني على عقد ما.
- هناك غياب للمعايير (وليس هناك مبادئ قانونية) تحدد الخصائص والتدريب التي يجب على أي خبير في الطب الشرعي بالكمبيوتر استيفائها.
- لم يجد الباحثون أي نوع من التدريب المنظم على التحليل للوسائط الرقمية.

التوصيات

هذا وقد المحنا فى ثنايا الكتاب الى عدد من التوصيات :

- يجب على المحامين النظر في كيفية تأثير صعود الذكاء الاصطناعي على واجباتهم الأخلاقية.
- يجب على المتخصصين القانونيين عمومًا استكشاف كيف يمكنهم الاستفادة من الفرصة الآن لتحسين تقديم الخدمات القانونية عبر العمليات والتقنيات الجديدة وضمان التطوير الأخلاقي للذكاء الاصطناعي وبذلك ، سيكونون أكثر قدرة على التنقل في التغييرات القادمة في السوق القانوني.

- يحب تطبيق سياسات صارمة للتحكم بالوصول للمعلومات والبيانات.
- يجب تطبيق سياسات المراجعة المستمرة للتأكد من جودة عملية الحماية والخصوصية.
- يجب إنشاء هيئة وطنية للمعلوماتية والحريات نظير المؤسسة الفرنسية التي تنظم وترعى شؤونها. فالتحول الى الرقمية لم يعد رفاهية ولا اختيارا بل هو تحدى اليوم وضرورة للغد و عملة اقتصاد المستقبل.
- التدريب المستمر والمتخصص لجميع القانونيين لمعرفة كيفية المضي قدما في جمع وتخزين الأدلة الإلكترونية والحفاظ على قيمتها الإثباتية أمام المحكمة عند الحاجة.
- يجب وضع إجراءات تنظيم لتقديم الأدلة الإلكترونية على المستوى الوطني والدولى.
- يجب تنفيذ بروتوكولات لحماية الحقوق الأساسية أثناء جمع الأدلة الإلكترونية وحفظها وعرضها .
- يجب الوفاء باتفاقية بودابست بشأن الجريمة السيبرانية (مجلس أوروبا) .
- يجب تحقيق تعاون أفضل بين الدول في مجال جمع الأدلة الإلكترونية وحفظها.
- يجب تحسين التواصل بين جميع الجهات الفاعلة المشاركة في إدارة الأدلة الإلكترونيةعلى وجه الخصوص ، لفهم أفضل بين القضاة والفنيين ، بالإضافة إلى حماية أعلى للخصوصية والبيانات الشخصية.

- يجب إنشاء وحدة رقمية داخل كل هيئة قضائية متعددة الخبرات الفنية والتقنية لتحليل الأدلة الرقمية ومعالجتها ، ومحللين شرعيين متخصصون في جرائم الإنترنت لحضور التحقيقات كخبراء محاكم الأسرة ومناقشة الجناة ومواجهتهم بالأدلة وتضم معمل لتحليل الأدلة ويعمل بالتنسيق مع مأموري الضبط القضائي وتبادل الخبرات ويضم مكتب تلقي البلاغات وشكاوى الأفراد والجهات آلياً عبر الإنترنت والتحقيق فيها بجدية وسرية تامة يضم أرشيف تحليلي للمعلومات والأدلة وسجلاً للسوابق القضائية والأدلة يعمل كدليل إرشادي يعين القضاة .
- يجب الـتدريب على الاكتشاف الإلكترونى في كليات الحقوق والتعليم القانوني على موضوعات تشمل:
  - احتضان مستقبل التكنولوجيا القانونية لتجنب التخلف عن الركب.
  - مواكبة الأشخاص الذين تمثلهم ثقافيًا وتقنيًا .
  - النماذج المالية الإبداعية والاستباقية في التقاضي .
  - التعاون والشفافية في الاكتشاف الإلكترونى.

وفي النهاية لا يخالجني شك في أن هذه الدراسة المتواضعة قد اعتراها بعض الأخطاء، وعذري فى ذلك انني بشر، يصيب ويخطأ، فالكمال لله وحده سبحانه، والخطأ والقصور هما من سمات الإنسان مهما أبدع وأتقن وجد واجتهد، وغاية ما ينشده كل باحث في عمله، هو تجويد هذا العمل، ومحاولة إتقانه فحسب، فإن كنت قد قاربت ما أنشده أو شارفت عليه فهذا فضل من الله ونعمه وحسبي ان اردد فى ذلك قوله تعالى " **وما توفيقي الا بالله** "، والشكر فيه لكل من علمنى حرفا ، وإن كانت الآخرى فحسبى أن أردد فى ذلك قوله تعالى "**وقل رب زدنى علما** " .

تم بحمد الله و فضله و توفيقه,,,,

المراجع

- **المراجع العربية:**

اولا :الكتب

— د/أسامة أحمد بدر ، حماية المستهلك في التعاقد الرقمي ، دراسة مقارنة ، دار الجامعة الجديد للنشر ، 2005

— أسامة المناعسة وآخرون ؛ د. هلالي عبداللاه أحمد ، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي . دراسة مقارنة ، الطبعة الأولى ، دار النهضة العربية . القاهرة ، 1997

— أيمن سعد عبد المجيد سليم ، التوقيع الرقمي ، دراسة مقارنة ، دار النهضة العربية ، 2005

— د/ أشرف جابر سيد ، الوجيز في أصول الإثبات ، دار النهضة العربية ، 2004 ، ص97

— جميل الشرقاوي، الإثبات في المواد المدنية ، دار النهضة العربية ،1976 ،ص41 وما بعدها ، سمير عبد السيد تناغو ، النظرية العامة في الإثبات ، منشأة المعارف بالإسكندرية ، 1999

— د. محمد المرسي زهرة ، الحاسب الرقمي ، الإثبات والقانون دراسة حول حجية. مخرجات الحاسب في الإثبات ، مكتبة سعيد عبد الله ، القاهرة ، ١٩٩٢

— د/ سحر عبد الستار إمام ، دور القاضي في الإثبات دراسة مقارنة، دون ناشر،2002

— د/عبد التواب مبارك ، الدليل الرقمي أمام القاضي المدني ، دار النهضة العربية ، بدون سنة نشر

— العالم الفقيه :ا.د/ عبد الرازق السنهوري ، الوسيط في شرح القانون المدني ، الجزء الثاني ، نظرية الالتزام بوجه عام ، طبعة 2004

— عبد المنعم فرج الصدة ،الإثبات في المواد المدنية ، مكتبة مكتبة مصطفي البابي الحلبي بمصر، 1954

— محمد حسين منصور ، الإثبات التقليدي والرقمي ، دار الفكر الجامعي بالإسكندرية ،2006

ثانيا : الرسائل العلمية

— د./عيسي غسان عبد الله الربضي ، القواعد الخاصة بالتوقيع الرقمي ، رسالة دكتوراه، ج.عين شمس

— د. عمر خالد محمد الزريقات ، عقد البيع عبر الإنترنت ، دراسة تحليلية ، رسالة دكتوراه، ج. عين شمس

— د/ عبد العزيز سعد بن دخيل الغانم ، المحكمة الرقمية ، دراسة تأصيلية ، رسالة دكتوراه ، جامعة نايف العربية للعلوم ، كلية العدالة الجنائية ، الرياض ، 2016

— د.محمد محمد سادات ، حجية التوقيع الرقمى فى الاثبات ، رسالة دكتوراه ، ج. المنصورة ، ٢٠١٠

— د/ نور خالد عبد المحسن العبد الرازق ، حجية المحررات والتوقيع الرقمي في الإثبات ، عبر شبكة الإنترنت، رسالة دكتوراه ، ج.عين شمس ، ٢٠٠٩

— د/ يوسف احمد النوافلة ، رسالة دكتوراه بعنوان "الإثبات الرقمي" ، كلية الحقوق ، جامعة الإسكندرية ، 2010

— محمد جميل إبراهيم ، اثر التقنيات الحديثة في مجال الدليل الكتابي ، رسالة دكتوراه ، كلية الحقوق ، جامعة الزقازيق .

ثالثا :الاوراق البحثية

— أحمد حمو، علاء عواد، ولاء عبد الله ، الأدلة الرقمية (الجوانب القانونية والتقنية) ، أوراق بحثية في القانون ومكافحة الفساد ، معهد الحقوق، جامعة بيرزيت، هيئة مكافحة الفساد ، فلسطين ، 2015

— Ken Chasse (1994) ، "السجلات التي تنتجها الكمبيوتر في إجراءات المحكمة" ، الملحق ياء لوقائع المؤتمر القانوني الموحد لكندا ، الاجتماع السنوي 1994 ، المحفوظ في:www.law.ualberta.ca/alri/ulc/94pro/ e94j.htm

— ا .د / براء منذر كمال عبداللطيف ، ا .م .د / أمير حسن جاسم ، المستندات الرقمية وحجيتها في الإثبات ، بحث مقدم للمؤتمر العلمي السنوي ، كلية الحقوق ، جامعة أسيوط ، بعنوان " العصر الرقمي" ، في الفترة من 12 إلي 13 إبريل 2016

- د.أمل فوزى أحمد ، بحث بعنوان " التحديات القانونية لخصوصية وأمن المعلومات الطبية الرقمية" منشور في المؤتمر الدولي الافتراضي الأول تحت عنوان : " دور المؤسسات في تحقيق التنمية المستدامة في ظل الاوبئة العالمية ، يومي 16 و15 يوليو 2020
- د.أمل فوزى أحمد ، بحث بعنوان " تحديات العدالة الرقمية أمام المحاكم المدنية " منشور بمجلة الدراسات والبحوث القانونية عدد جوان 2020.
- د/أمل فوزى أحمد ،بحث بعنوان " الامن الانسانى فى ظل تحديات التحول الى الرقمية لمستقبل حقوق الانسان " ، الملتقى الدولى الموسوم " الأمن الإنسـاني في ظل التحديات العالمية المعاصرة " ، 9 و10 يناير 2021.
- د/أمل فوزى أحمد ،بحث بعنوان " المهارات الفنية والقانونية لإدارة الخصومة القضائية رقميا" ، المؤتمر العلمي الخامس (الافتراضي) ، كلية الحقوق جامعة السلطان قابوس ، " نظم التقاضي وتحديث قواعد الاثبات "تطوير نظم التقاضي وتحديث قواعد الإثبات" ، ٢٢ ديسمبر ٢٠٢٠.
- د/أمل فوزى أحمد ،بحث بعنوان " آليات فعالة للتحول الآمن بالنظم القضائية الى الرقمية" ، المؤتمر العلمي الخامس (الافتراضي) ، كلية الحقوق جامعة السلطان قابوس ، " نظم التقاضي وتحديث قواعد الاثبات "تطوير نظم التقاضي وتحديث قواعد الإثبات" ، ٢٢ ديسمبر ٢٠٢٠.
- د/أمل فوزى أحمد ،بحث بعنوان " معالجات تشريعية لضبط الحقوق والحريات فى البيئة الرقمية" المؤتمر العلمى السادس , القانون والشائعات ,كلية الحقوق ,جامعة طنطا ,23-24 ابريل 2019.
- د/أمل فوزى أحمد ،بحث بعنوان "الإكتشاف الإلكترونى ، والوصول الأسرع للعدالة مزايا أم تحديات؟" ، المؤتمر الدولى الأول ، تحت عنوان " التحولات الرقمية : التأثيرات والتحديات " ، كلية العلوم القانونية ،والاقتصادية ، والاجنماعية ، بتطوان ، جامعة عبد المالك السعدى ، المغرب ، يومى 9و10 يونيو 2021.
- د/أمل فوزى أحمد،بحث بعنوان " الأدلة الرقمية في الإثبات بين معايير القبول وأمن المعلومات "، منشور بالمجلة الدولية للاجتهاد القضائي : العدد الثاني يوليو – تموز 2021 ،المجلد 1 –المركز_الديمقراطي_العربي المانيا- برلين .
- د/أحمد محمود أحمد ، د. إسلام إبراهيم شيحا ، القاضي ووسائل التواصل االجتماعي ، المؤتمر العلمي الخامس (الافتراضي) ، كلية الحقوق جامعة السلطان قابوس ، " نظم

التقاضي وتحديث قواعد الاثبات "تطوير نظم التقاضي وتحديث قواعد الإثبات" ، ٢٢ ديسمبر ٢٠٢٠ .

— د/ أحمد محمد عبدالرحمن، نظرة حول نظام التقاضي الالكتروني في مصر، بحث مقدم للمؤتمر العلمي الحادي عشر" الاتجاهات الحديثة في القانون الإجرائي" ، كلية الحقوق .،جامعة أسيوط ، مارس 2017.

— بدر بن عبدالله الجعفري، بحث بعنوان الإثبات الرقمي في المنازعات التجارية، مقدم للمتلقي العدلي "وسائل الإثبات" الذي نظمته الغرفة التجارية بمدينة الأحساء ، المملكة العربية السعودية، يناير 2013

— أ.د. عابد فايد عبد الفتاح فايد ، القاضي والتنازع بين الأدلة الكتابية التقليدية والرقمية . دراسة مقارنة بين القانون الفرنسي وقوانين بعض الدول العربية ، المؤتمر العلمي الخامس (الافتراضي) ، كلية الحقوق جامعة السلطان قابوس ، " نظم التقاضي وتحديث قواعد الإثبات "تطوير نظم التقاضي وتحديث قواعد الإثبات" ، ٢٢ ديسمبر ٢٠٢٠

— د. علي بن سعيد بن حمود البداعي ، التقاضي عن بعد ، المؤتمر العلمي الخامس (الافتراضي) ، كلية الحقوق جامعة السلطان قابوس ، " نظم التقاضي وتحديث قواعد الاثبات "تطوير نظم التقاضي وتحديث قواعد الإثبات" ، ٢٢ ديسمبر ٢٠٢٠.

— د. محمد كمال شاهين ، حجية الدليل الرقمي في الإثبات الجنائي . دراسة مقارنة ، المؤتمر العلمي الخامس (الافتراضي) ، كلية الحقوق جامعة السلطان قابوس ، " نظم التقاضي وتحديث قواعد الإثبات "تطوير نظم التقاضي وتحديث قواعد الإثبات" ، ٢٢ ديسمبر ٢٠٢٠

— د. هشام عبد السيد الصافي ، القضاء الإداري المصري والتكنولوجيا الحديثة ، مقال نشر في مجلة جيل الأبحاث القانونية المعمقة ،العدد 17.

— د/ الأنصاري حسن النيداني، القاضى والوسائل الالكترونية الحديثة، دار الجامعة الجديدة , بدون سنة نشر

— د/ راشد بن حمد البلوشي ، ورقة عمل يقدمها مقدمه الي المؤتمر الدولي الاول حول"حماية امن المعلومات و الخصوصيه في قانون الانترنت" ، برعاية الجمعيه الدوليه لمكافحة الاجرام السيبيري بفرنسا ، الفتره من 2 الى 4 يونيو 2008 القاهرة جمهورية مصر العربية

— د/ سيد احمد محمود ، بحث بعنوان "نحو الكترونية القضاء المدنى " ، مؤتمر القانون والتكنولوجيا ،كلية الحقوق ،جامعة عين شمس ، ديسمبر 2017.

— د/فاطمةعادل سعيد "التقاضي عبر وسائل التكنولوجيا والاتصال الحديث " , بحث مقدم الى مؤتمرالقانون واللتكنولوجيا – كلية الحقوق – جامعةعين شمس , فى الفترة من 8 الى 10 ديسمبر 2017.
— ماريا فيرونيكا بيريزAsinari– المجلة الدولية للقانون الحاسبات و ، Technology ، Vol 18، No 2، 2004.
— المستشار د/ ياسر أحمد بدر ، الاتجاهات الحديثة في التصديق الرقمي ، بحث مقدم للمؤتمر العلمي السنوي الحادي عشر ، كلية الحقوق ، جامعة أسيوط ، بعنوان الاتجاهات الحديثة في القانون الإجرائي ، في الفترة من 29 :30/ 3/2017
— المهندس/ سعيد عطا الله, ما الفرق بين الأمان والخصوصية , مقال منشور بتاريخ :2020/5/14

رابعا : احكام محكمة النقض

— الطعن رقم 17689لسنة 89 قضائية الدوائر التجارية – جلسة 10/3/2020.
— الطعن رقم 17051 لسنة 87 قضائية الدوائر التجارية – جلسة 28 /3/2019.
— الطعن رقم 12415 لسنة 87 قضائية الدوائر التجارية – جلسة 23/12/2018.

- **المراجع الاجنبية:**

A. Research paper :

- "The transformation of civil justice to digital advantages between difficulties and challenges " , BISKRA UNIVERSITY - FACULTY OF LAW AND POLITICAL SCIENCES Laboratory impact of jurisprudence on the dynamics of legislation, Jurisprudence Journal -- Vol 12 – (Special Issue) – September 2020
- "Intellectual property and artificial intelligence Reality & the Future", BISKRA UNIVERSITY - FACULTY OF LAW AND POLITICAL SCIENCES Laboratory impact of jurisprudence on the dynamics of legislation, Jurisprudence Journal -- Vol 35 – (Special Issue - S N 42) – 19 January 2021.
- ADAM I. COHEN, DAVID J. LENDER, ELECTRONIC, DISCOVERY, PRACTICE, GUIDELINES, p2-37
- AHIMA. "E- Discovery Litigation and Regulatory Investigation Response Planning: Crucial Components of Your Organization's Information and Data Governance Processes." Journal of AHIMA 84, no.11 (November–December 2013): expanded web version , p 1-91 .
- Difference Between Security and Privacy من موقع: www.differencebetween.net، 2019-3-7 اطّلع عليه بتاريخ
- Dimick, Chris. "E-Discovery: Preparing for the Coming Rise in Electronic Discovery Requests." Journal of AHIMA 78, no. 5 (May 2007): 24–29. Federal Rules of Civil Procedure http://www.law.cornell.edu/rules/frcp
- Ediscovery And Digital Forensics , Solving Legal And Regulatory Issues , P1-6 , Cyber@Bsigroup.Com , Bsigroup.Com
- e-Discovery: What Litigation Lawyers Need to Know , Risk Management Practice Guide of Lawyers Mutual, LAWYERS MUTUAL LIABILITY INSURANCE COMPANY OF NORTH CAROLINA
- Helmut Rümann، Electronic Documents. Security and Authenticity، Electronic Technology and Civil Procedure- New Paths to Justice from Around the World، Springer، 2012، p.235.
- HIV.gov، The Difference between Security and Privacy and Why It Matters to Your Program، من موقع: www.hiv.gov، 7-3- اطّلع عليه بتاريخ 2019

- http://www.abanet.org/litigation/discoverystandards/2004civildiscoverystandards.pdf).
- https://bok.ahima.org/doc?oid=107115#.YDekLujXLx4
- Jay Thornton, (Cost, Accuracy, and subjective fairness in legal information technology: a response to technological due process critics), New York university law review, December 2016, Vol.91, p.
- Koulika Arnaud NIKIEMA، La preuve dans le contentieux du cyberespace ،Université Gaston Berger de Saint Louis du Senegal - Master pro (DESS)Droit du cyberespace 2011،p6
- Legal Technology Vision Towards the digital transformation of the legal sector , Legal Technology Cluster Committee , Singapore Academy of Law , p33
- Mike L. Bridenback, Consultant ,Study of State Trial Courts Use of Remote Technology Final Report, National Association for Presiding Judges and Court Executive Officers, April 2016, p9-27
- Osama Ahmed Attalla , Is The Legal Protection Of Digital Privacy Enough In Egypt" ? Protection Of Digital Data Privacy ", A Paper Submitted For The Conference Of Cyber Crimes , National Institute Of Intellectual Property April 2020 .
- Sophia BINET، L'utilisation des nouvelles technologies dans le procès civil : Vers une procédure civile intégralement informatisée، p65.
- http://www.abanet.org/litigation/discoverystandards/2004civildiscoverystandards.pdf).
- Valérie Sédallian: L´archivage de l´acte électronique, juriscom.net,8 juillet 2002, le sur sit: http://www.juriscom.net..
- Walker, Janet, and Garry D. Watson. "New Trends in Procedural Law: New Technologies and the Civil, Litigation Process." Hastings International and Comparative Law Review 31.1 (2008), http://www.delmarlearning.com/companions/content/1401824293/guides/CH6.
- What's the Difference Between Privacy and Security?، من موقع: www.globalsign.com، 2019-3-7 اطّلع عليه بتاريخ
- www.dlapiperdataprotection.com., Data Protection Laws of the World
- Zheng, Tina, "Advanced Surveillance Technologies: Privacy and Evidentiary Issues" (2016). Cornell Law School J.D. Student Research Papers. 37, p1-10, http://scholarship.law.cornell.edu/lps_papers/37

Sites:

- https://sitcegypt.org/?p=1425www.lawyersmutualnc.com
- www.hiv.gov، اطّلع عليه بتاريخ 7-3-2019
- www.globalsign.com، اطّلع عليه بتاريخ 7-3-2019
- www.differencebetween.net، اطّلع عليه بتاريخ 7-3-2019
-of-digital-evidence.html
- ISO / IEC 27037 ؛ Cybercrime Module 4 on Introduction to Digital Forensics
- https://www.unodc.org/e4j/en/cybercrime/module-6/key-issues/handling
- https://www.unodc.org/e4j/en/cybercrime/module-6/key-issues/handling-of-digital-evidence.html
- https://www.unodc.org/e4j/en/cybercrime/module-6/key-issues/digital-evidence-admissibility.html
- https://www.ukessays.com/essays/criminology/presenting-digital-evidence-to-court-criminology-essay.php
- https://www.ukessays.com/essays/criminology/presenting-digital-evidence-to-court-criminology-essay.php
- https://www.ukessays.com/essays/criminology/presenting-digital-evidence-to-court-criminology-essay.php
- https://www.tandfonline.com/doi/full/10.1080/17579961.2020.18https://www.tandfonline.com/doi/abs/10.1080/136008604200022350 8?src=recsys&journalCode=cirl20

- https://www.tandfonline.com/doi/full/10.1080/15567280701418049?src=recsys
- https://www.tandfonline.com/doi/full/10.1080/15567280701418049?src=recsys
- https://www.tandfonline.com/doi/abs/10.1080/1360086042000223508?src=recsys&journalCode=cirl20
- https://www.tamimi.com/law-update-articles/admissibility-and-reliability-of-electronic-evidence-before-qatari-courts/
- https://www.sciencedirect.com/science/article/pii/B978159749643800016X
- https://www.salamatech.org/الخصوصية-من-منظور-حقوق-الإنسان/
- https://www.sal.org.sg/Resources-Tools/Legal-Technology-Vision
- https://www.researchgate.net/publication/327644306_Digital_Forensics_Review_of_Issues_in_Scientific_Validation_of_Digital_Evidence
- https://www.relativity.com/blog/the-end-of-an-e-discovery-era-judge-scheindlins-law-from-zubulake-to-today/,
- https://www.mailxaminer.com/blog/admissibility-of-electronic-evidence-in-court/
- https://www.logikcull.com/what-is-ediscovery-software
- https://www.logikcull.com/guide/introduction-to-ediscovery-basics
- https://www.lita-lb.org/archive/51-dossier-médical-electronique.html
- https://www.lexology.com/library/detail.aspx?g=29828d6d-8396-4070-9424-05ac2e0ecfae
- https://www.lexology.com/library/detail.aspx?g=29828d6d-8396-4070-9424-05ac2e0ecfae

- https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT 00 0000404810last visited 22 October 2017 .
- https://www.lawtechnologytoday.org/2021/05/working-from-home-7-cybersecurity-tips-to-protect-your-data
- https://www.lawtechnologytoday.org/2021/05/small-business-cyber-security-testing-measures
- https://www.lawtechnologytoday.org/2021/05/can-tech-advances-fuel-a-medical-malpractice-crisis
- https://www.lawtechnologytoday.org/2021/05/advantages-of-having-a-virtual-assistant-in-your-team
- https://www.lawtechnologytoday.org/2021/02/using-artificial-intelligence-to-improve-law-firm-performance
- https://www.lawtechnologytoday.org/2020/12/three-key-questions-to-ask-before-collecting-remotely/
- https://www.lawtechnologytoday.org/2020/11/techreport-2020-litigation-tar
- https://www.lawtechnologytoday.org/2020/09/legal-teams-should-seek-forward-looking-ai-technology الموقع علي دخول آخر تاريخ)/ (2020/9/22
- https://www.lawtechnologytoday.org/2020/08/make-better-choices-with-legal-data(2020/9/22 الموقع علي دخول آخر تاريخ)/
- https://www.lawtechnologytoday.org/2020/08/how-to-effectively-manage-data-breach-risks-from-third-parties علي دخول آخر تاريخ)/ (2020/9/22 الموقع
- https://www.lawtechnologytoday.org/2020/02/abbyy-to-showcase-digital-intelligence-solutions-to-transform-legal-operations-at-the-american-bar-association-techshow-2020/

- https://www.lawtechnologytoday.org/2020/02/5-ways-to-retake-control-of-your-document-intensive-business-processes
- https://www.lawtechnologytoday.org/2019/07/client-driven-innovation-the-future-of-legal-technology/
- https://www.lawtechnologytoday.org/2019/06/upskill-litigation-support-managers-to-add-value-firm-wide
- https://www.lawtechnologytoday.org/2019/06/can-legal-tech-education-help-move-the-needle
- https://www.lawtechnologytoday.org/2019/05/digital-transformation-key-implications-for-law-firm-technology-services-and-offerings
- https://www.lawtechnologytoday.org/2019/04/e-discovery-using-agile
- https://www.lawtechnologytoday.org/2019/04/artificial-intelligence-will-change-e-discovery-in-the-next-three-years
- https://www.lawtechnologytoday.org/2018/05/six-questions-you-must-ask-before-buying-e-discovery-software
- https://www.lawtechnologytoday.org/2017/08/e-discovery-request-youre-requesting/
- https://www.lawtechnologytoday.org/2014/10/predictive-coding-for-rookies-e-discovery-in-the-courtroom
- https://www.lawteacher.net/free-law-essays/commercial-law/relevancy-and-admissibility-of-electronic-law-essays.php
- https://www.lawgazette.co.uk/news/law-enforcers-struggle-with-electronic-evidence-challenges-/5066471.article
- https://www.larkinhoffman.com/files/OTHER/bjd_ppp_elecdis.pdf
- https://www.google.com/search?sxsrf=ALeKk03chjd_CNkdk1Fnsot6owkUFOs-

4Q:1622449002937&q=Digital+Evidence+and+Computer+Crime:+Forensic+Science,+Computers+and+the+Internet&stick=

- https://www.exterro.com/basics-of-e-discovery/e-discovery-process
- https://www.exterro.com/basics-of-e-discovery
- https://www.ehealthsa.com/archives/2261
- https://www.crime-scene-investigator.net/admissibilitydigitaleveidencecriminalprosecutions.html
- investigator.net/admissibilitydigitaleveidencecriminalprosecutions.html
- https://www.crime-scene-investigator.net/admissibilitydigitaleveidencecriminalprosecutions.html
- https://www.consumersinternational.org/news-resources/news/arabic-news/blog-will-gdpr-be-the-global-standard-for-data-protection-arabic/ للائحة العامة لحماية البيانات: هل ستكون المعيار العالمي لحماية البيانات؟
- https://www.consumersinternational.org/news-resources/news/arabic-news/blog-will-gdpr-be-the-global-standard-for-data-protection-arabic/ للائحة العامة لحماية البيانات: هل ستكون المعيار العالمي لحماية البيانات؟
- https://www.cc.gov.eg/judgment_single?id=111398859&ja=2754htt
- https://www.cc.gov.eg/judgment_single?id=111387601&&ja=270764
- https://www.bcs.org/content-hub/presenting-digital-evidence-to-court
- https://www.atlanticdf.com/blog/2017/12/18/admissibility-of-digital-evidence-in-court/

- https://www.atlanticdf.com/blog/2017/12/18/admissibility-of-digital-evidence-in-court/
- https://www.arageek.com/الخصوصية-والأمان-بين-الفرق-ما/
- https://www.aiim.org/what-is-ediscovery
- https://v1.lawgazette.com.sg/2001-11/Nov01-focus2.htm(تاريخ آخر دخول علي الموقع 22/9/2020)
- https://taqadom.aspdkw.com/الصحية-المعلومات-أمن/
- HTTPS://TAQADOM.ASPDKW.COM / تاريخ احر, أمن-المعلومات-الصحية/ دخول: 28/6/2020
- https://sitcegypt.org/?p=1425 تشريعات الخصوصية الرقمية/
- https://phys.org/news/2015-03-digital-forensics.html
- https://nydailyrecord.com/2013/07/22/an-interview-with-laura-zubulake/,
- https://mobile.emirates.com/MobileTermsConditions/jo/arabic/what_sensitive_personal_data_might_you_require_or_hold.xhtml?lang=ar_JO
- HTTPS://ME.KASPERSKY.COM/ENTERPRISE-SECURITY/HEALTHCARE
- https://linkitsys.com/ar/ ملف-المريض-السجل-الطبى-للمريض/ أمن البيانات الصحية في الأنترنت السحابي
- https://library.ahima.org/searchresults?fqa=CategoryIdsAllHierarchical|{5B64421A-6F43-4FC1-B278-9EA38EA92210}&s=3&v=1&num=10
- https://hi-in-ksa.com/2015/12/20/قواعد-بياناتا-ومجلات-علمية-في-المعلوم/
- https://hi-in-ksa.com/2013/07/08/
- https://en.wikipedia.org/wiki/Zubulake_v._UBS_Warburg,
- https://en.wikipedia.org/wiki/Electronic_discovery

- https://en.wikipedia.org/wiki/Digital_evidence Tech. 5 (2011)
- https://en.wikipedia.org/wiki/Digital_evidence
- https://economictimes.indiatimes.com/news/politics-and-nation/courts-can-rely-on-electronic-records-without-certificate-supreme-court/articleshow/62777759.cms
- https://economictimes.indiatimes.com/news/politics-and-nation/courts-can-rely-on-electronic-records-without-certificate-supreme-court/articleshow/62777759.cms
- https://docplayer.net/9703973-Electronic-case-files-system-user-s-manual.html(2020/9/22 تاريخ آخر دخول علي الموقع)
- https://docplayer.net/680438-Instant-messaging-security.html
- https://docplayer.net/21648942-Second-amended-order-designating-all-cases-e-file-and-setting-forth-certain-requirements-in-e-file-cases.html تاريخ آخر دخول علي الموقع) (2020/9/22
- https://docplayer.net/14451754-Electronic-forms-processing-eforms.html2020/9/22 تاريخ آخر دخول علي الموقع)
- https://docplayer.net/13527036-File-how-to-transmit-civil-court-documents-by-fax-for-filing-in-court-registries-in-b-c-transmitting-by-fax-court-services-court-services-branch.html تاريخ)
- https://docplayer.net/13165153-Making-reliable-web-services-message-exchanges-secure-and-tamper-proof-alan-j-weissberger-data-communications-technology-aweissberger-sbcglobal.html(2020/9/22 تاريخ آخر دخول علي الموقع)
- https://docplayer.net/10509033-Content-management-for-courts-improve-court-operations-by-reducing-costs-speeding-response-times-and-simplifying-paper-intensive-processes.html

- https://digitalcommons.osgoode.yorku.ca/cgi/viewcontent.cgi?article=2378&context=scholarly_works
- https://cloudnine.com/ediscoverydaily/case-law/ediscovery-history-a-look-back-at-zubulake/,
- https://ci.security/resources/news/article/3-methods-to-preserve-digital-vidence-for-computer-forensics
- https://cdslegal.com/knowledge/the-basics-what-is-e-discovery/
- https://bok.ahima.org/doc?oid=107115#.YDekLujXLx4 تاريخ آخر دخول 21/2/2021 علي الموقع
- https://bok.ahima.org/doc?oid=107115#.YDekLujXLx4
- https://blog.signaturit.com/en/electronic-evidence-and-its-admissibility-in-court
- https://articles.forensicfocus.com/2017/06/29/an-introduction-to-challenges-in-digital-forensics/
- https://ar.wikipedia.org/wiki/قانون_خصوصية_المعلومات
- https://aitnews.com/2018/05/27/اللائحة-العامة-لحماية-البيانات-gdpr/
- http://www.worldcat.org/title/electronic-technology-and-civil-procedure-new-paths-to-justice-from-around-the-world/oclc/773670695
- http://www.stephenmason.eu/articles/electronic-evidence.html
- http://www.law.georgetown.edu/library/collections/catalog/new-titles/august2012.cfm(تاريخ آخر دخول علي الموقع : 2021/1/8)
- http://www.jurisdiction.com/ecom4.htm
- http://www.camerapenale-bologna.org/codice_procedura_penale/codice_di_procedura_penale_index.htm#cpbo.
- http://www.alkhaleej.ae/alkhaleej/page/aaf7afa4-f9ac-4974-ab6e-cdb1ab5102b8#sthash.jTiWe8R0.dpuf

- http://www.alkhaleej.ae/alkhaleej/page/aaf7afa4-f9ac-4974-ab6e-cdb1ab5102b8
- http://www.adminet.com/code/index-CPROCPEL.html
- http://aurora.turiba.lv/editor/Conference14/vBook/proceeding/pages/EN030_Simeblyte_Nemeiksis/EN030_Simeblyte_Nemeiksis.htm
- http.//www.healthvault.com
- www.law.ualberta.ca/alri/ulc/94pro/ e94j.htm
- (https://www.tandfonline.com/doi/full/10.1080/15567280701418049?src=recsys-
- https://www.getapp.com/legal-law-software/electronic-discovery/
- https://linkitsys.com/ar/أمن البيانات /ملف-المريض-السجل-الطبى-للمريض الصحية في الأنترنت السحابي
- https://library.ahima.org/doc?oid=301993#.YL9d1_nXIak

الفهرس

المحتوى	رقم الصفحة
مقدمة	**7**
المبحث الأول: الاكتشاف الإلكترونى	**11**
المطلب الأول: ماهية الاكتشاف الإلكترونى و الإدارة الذكية للمعلومات	**13**
المطلب الثانى: متطلبات الاكتشاف الإلكترونى	**22**
المطلب الثالث: تحديات الاكتشاف الإلكترونى	**25**
المطلب الرابع: التخطيط الناجح الاكتشاف الإلكترونى	**31**
المطلب الخامس: الذكاء الاصطناعي والاكتشاف الإلكترونى	**38**
المبحث الثانى : الأدلة الرقمية	**44**
المطلب الأول : ماهية الأدلة الرقمية	**48**
المطلب الثاني : متطلبات الإثبات بالأدلة الرقمية	**57**
المطلب الثالث : أنواع الأدلة الرقمية	**63**
المطلب الرابع : تحديات قبول الأدلة الرقمية	**88**
المطلب الخامس: موقف النظم القضائية المقارنة	**93**
الخاتمة والنتائج	**103**
التوصيات	**105**
المراجع	**107**

Electronic Discovery & Digital Evidence Authority In proof between The challenges of acceptance and information security

Prepare:

Dr. amal Fawzy Ahmed

PhD in Law/Faculty of Law/Ain Shams University

Head of the Information Technology Unit, Faculty of Technical Education, University of Halwan

2022

المركز الديمقراطي العربي
للدراسات الإستراتيجية والسياسية والإقتصادية
D.A.C