



المركز الديمقراطي العربي
برلين - ألمانيا

الإيداع الرقمي وأمن المعلومات

تأليف:
د. أمل فوزى أحمد عوض



2022



الإيداع الرقمي وأمن المعلومات



المركز الديمقراطي العربي
برلين - ألمانيا



Democratic Arab Center
Berlin - Germany

Digital Deposit & Information Security



VR . 3383 – 6603 B

DEMOCRATIC ARABIC CENTER
Germany, Berlin 10315 Gensinger- Str. 112

<http://democraticac.de>

TEL: 0049-CODE

030-89005468/030-898999419/030-57348845

MOBILTELEFON: 0049174274278717

النـاشـر:

المركز الديمقراطي العربي
للدراستات 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
للدراستات الاستراتيجية والسياسية والاقتصادية ألمانيا/برلين

Tel: 0049-code Germany

030-54884375

030-91499898

030-86450098

البريد الإلكتروني

book@democraticac.de





المركز الديمقراطي العربي

للدراستات الاستراتيجية، الاقتصادية والسياسية

Democratic Arab Center
for Strategic, Political & Economic Studies

الكتاب : الإيداع الرقمي 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 – 6603. B

الطبعة الأولى

شباط / فبراير 2022 م

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



الإيداع الرقمي & أمن المعلومات

Digital Deposit & Information Security



اعداد /

و.أمل فوزى أحمد عوض

دكتوراه فى القانون / كلية الحقوق / جامعة عين شمس

رئيس وحدة تكنولوجيا المعلومات - كلية التربية الفنية - جامعة حلوان

2022

الملخص :

الأصل بالنسبة لرفع الدعوي أن يتم رفعها بواسطة ورقة تسمى صحيفة افتتاح الدعوي أو عريضة الدعوي، وهذه الورقة تودع قلم كتاب المحكمة المختصة بعد أن يتم استيفاء جميع بياناتها. أما رقميا تعتبر الدعوي مرفوعة إلي المحكمة بناء علي قيام المدعي بمليء الطلب المعد لذلك والموجود علي الموقع الرقمي للمحكمة (الصحيفة الرقمية) ، وهو الأمر الذي يتطلب ضرورة معرفة الآلية التي سيتم بها الإيداع الرقمي لصحيفة الدعوي ؟؟؟ ، و الكيفية التي يتم بها إجراءات المطالبة القضائية عبر الوسائط الرقمية؟؟؟؟ ، وكذلك معرفة ماهي الآثار المترتبة على المطالبة القضائية؟؟؟ ، وجميع ما سبق لابد ان يتم فى ظل أمن معلوماتى فكيف سيكون ذلك؟؟؟؟ ، وما هو موقف النظم القضائية المقارنة؟؟؟

الكلمات المفتاحية :

الإيداع الرقمي - المطالبة القضائية - الوسائط الرقمية - أمن المعلومات - التداعى -

الخصومة القضائية .

Summary:

The original for filing the case should be filed by a paper called the opening newspaper of the suit or the petition of the suit, and this paper deposits the registry of the competent court book after all its statements have been completed in accordance. As for digitally, the case is considered to be filed with the court based on the plaintiff's fill out the request prepared for this and located on the digital website of the court (digital newspaper), which requires the need to know the mechanism by which the digital filing of the lawsuit newspaper will be made??? How is the judicial claim process done through digital media????? And also find out what the implications of the judicial claim are??? And all of the above must be done in the light of the security of my information, how will that be???? And what is the stop of comparative judicial systems???

Keywords:

Digital filing – judicial claim – digital media – information security – collapse – judicial litigation.

Résumé:

L'original pour le dépôt de l'affaire doit être déposé par un journal appelé le journal d'ouverture de la poursuite ou la requête de la poursuite, et ce document dépose le greffé du livre du tribunal compétent après que toutes ses déclarations ont été complétées conformément. En ce qui concerne le numérique, l'affaire est considérée comme étant déposée auprès du tribunal sur la base du fait que le demandeur a rempli la demande préparée à cet effet et située sur le site Web numérique du tribunal (journal numérique), ce qui nécessite la nécessité de connaître le mécanisme par lequel le dépôt numérique du journal de la poursuite sera effectué??? Comment se déroule le processus de réclamation judiciaire par le biais des médias numériques????? Et découvrez également quelles sont les implications de la réclamation judiciaire??? Et tout ce qui précède doit être fait à la lumière de la sécurité de mes informations, comment cela sera-t-il???? Et qu'est-ce que l'arrêt des systèmes judiciaires comparés???

Mots-clés:

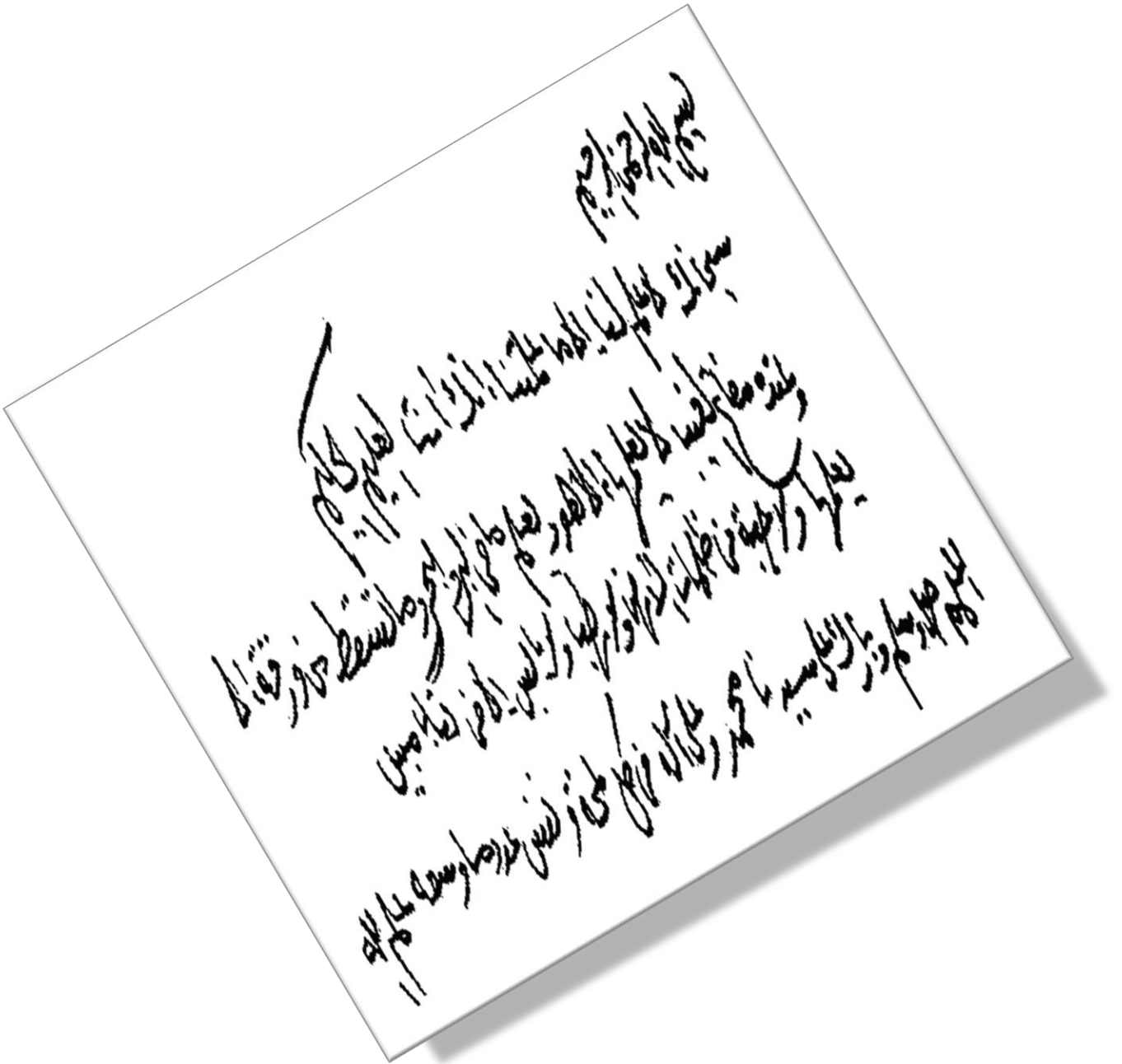
Dépôt numérique - réclamation judiciaire - médias numériques - sécurité de l'information - effondrement - litige judiciaire.

Zusammenfassung:

Das Original für die Einreichung des Falles sollte von einem Papier eingereicht werden, das als Eröffnungszeitung der Klage oder der Petition der Klage bezeichnet wird, und dieses Papier hinterlegt das Register des zuständigen Gerichtsbuchs, nachdem alle seine Erklärungen gemäß Was die digitale Belange betrifft, so gilt der Fall als beim Gericht eingereicht, basierend auf dem dafür vorbereiteten antrag des Klägers, der sich auf der digitalen Website des Gerichts (digitale Zeitung) befindet, was die Notwendigkeit erfordert, den Mechanismus zu kennen, mit dem die digitale Einreichung der Klagezeitung erfolgt???. Wie erfolgt das gerichtliche Klageverfahren über digitale Medien?????? Und finden Sie auch heraus, was die Auswirkungen der gerichtlichen Klage sind???. Und all das oben Genannte muss im Lichte der Sicherheit meiner Informationen geschehen, wie wird das sein???? Und was ist die Station vergleichender Rechtssysteme???

Schlüsselwörter:

Digitale Einreichung – Gerichtlicher Anspruch – Digitale Medien – Informationssicherheit – Zusammenbruch – Gerichtsverfahren.



إهداء

إذا جاء فضلك الله وأنعمه تّرا

فيكون الحمد والشكر يسعي

وأهدمي الجهد والإجتهاد صبرا

لأبي ثم أمي عرفانا وليس ردأ

وقبلهم الرسول حبيبا وفخرا

به التمام والسند فضلا وكراما

□

□ شَر

□ الشكر موصولا لك من علمني حرفا ما دعت حيا.....

المقدمة

إن الطريقة التي يتم بها إدخال تكنولوجيا المعلومات في التقاضي¹ تختلف من دولة لأخرى² لاختلاف النظام القضائي والفلسفة الإجرائية السائدة ، ولعل أبرز مثال لذلك دور المحكمة في القضية المدنية ففي بعض النظم يكون للمحكمة دور أساسي وإيجابي بداية من مرحلة تقديم صحيفة الدعوي إلي المحكمة المختصة وإعلانها ثم انعقاد الجلسات انتهاء بصدور حكم في الدعوي، فهنا تكون المحكمة مسؤولة عن ضمان التوازن والعدالة الإجرائية بين الخصوم والتأكد من سلامة الإجراءات والاتصال بين المحكمة والخصوم وبين الخصوم أنفسهم أثناء عملية تبادل المذكرات علي الجانب الآخر فإن هناك بعض الدول التي يعد فيها الاتصال الفعلي للمحكمة بالقضية أو بصورة أدق بداية مباشرة سلطاتها في الرقابة وإدارة الدعوي هي مرحلة انعقاد الجلسات، فتعتبر كافة الإجراءات التي تسبق المحاكمة إجراءات غير رسمية وتخضع لإرادة الخصوم ، فإن اختلاف دور المحكمة يعكس بالضرورة اختلافا في أسلوب إدارة الإجراءات وإمكانية إدخال تكنولوجيا³ في التقاضي ومدى إمكانية ذلك الإدخال⁴.

1 راجع في ذلك :

Timothy J. Chorvat and Laura E. Pelanek , Electronically Stored Information in Litigation Source, The Business Lawyer , November 2010, Vol. 66, No. 1 (November 2010), pp. 183- 189 , Published by: American Bar Association Stable , , URL: <https://www.jstor.org/stable/25758532>

2 راجع في ذلك : د/ فاطمة عادل سعيد ، التقاضي عبر وسائل التكنولوجيا والاتصال الحديث ، التقاضي عبر وسائل التكنولوجيا والاتصال الحديث، بحث مقدم لمؤتمر "القانون والتكنولوجيا ، كلية الحقوق ، جامعة عين شمس ، ديسمبر 2017 ، الجزء الأول ، ص 359 وما بعدها .

3 راجع التفاصيل التقنية للإجراء الإلكتروني بمراحل الخصومة "برمجة الدعوي إلكترونيا ، د/ محمد صابر احمد ، دور الحاسب الآلي في تيسير إجراءات التقاضي ، دور الحاسب الآلي في تيسير إجراءات التقاضي " ، رسالة دكتوراه ، كلية الحقوق ، جامعة طنطا ، 2012 ، ص 182 وما بعدها .

4 راجع في ذلك :

ويتبدى ذلك الاختلاف في مختلف مراحل القضية المدنية، فيتشكل الجانب الموضوعي لها من ادعاء الخصوم حق أو مركز قانوني معين (الدعوي)، أما الجانب الإجرائي لها أي الخصومة هي الموضوع الرئيسي الذي تنصب عليه دراسة إدخال تكنولوجيا المعلومات إلي إجراءات التقاضي حيث إنها مجموعة الإجراءات القضائية المتتالية ، ويقوم بها كلا من القاضي وأعدائه والخصوم ومن يمثلهم وفقا للنظام الذي يقرره قانون المرافعات¹ وتبدأ بالمطالبة القضائية وصولا للحكم في موضوع الدعوي ، والخصومة في سبيل تحقيقها لغايتها وهو الوصول لحكم فاصل في الدعوي ، فالدعوى تمر بثلاث مراحل هي: مرحلة افتتاح الخصومة وتبدأ بإيداع صحيفة المطالبة القضائية ثم إعلانها للخصم الآخر وتحديد موعد للجلسة الأولى وبهذا تنعقد الخصومة، ثم مرحلة سير الخصومة (وهي المرحلة التي تنصب بصفة رئيسية علي سير الجلسات وإدارتها ومرافعات الخصوم والأدلة) ، وأخيرا مرحلة صدور الحكم باعتبارها ختام الخصومة .

وفي كل مرحلة من المراحل الثلاث السابق نكرها يمكن استخدام تكنولوجيا المعلومات مما يؤدي إلي تسريع عملية التقاضي ومحاولة تقليل العراقيل التي تعترضها بطبيعة الحال باعتبارها قائمة علي الشكلية وذلك باستخدام الوسائل التكنولوجية ، و لعل من أهم المراحل التي يمكن دراسة تطبيق تكنولوجيا المعلومات فيها هي مرحلة ما قبل انعقاد الخصومة، فتتضمن هذه المرحلة المطالبة القضائية وإيداع صحيفة الدعوى لدي المحكمة ومن ثم إعلانها للخصم الآخر،

Timothy J. Chorvat and Laura E. Pelanek , Electronically Stored Information in Litigation Source, The Business Lawyer , November 2010, Vol. 66, No. 1 (November 2010), pp. 183- 189 , Published by: American Bar Association Stable , , URL: <https://www.jstor.org/stable/25758532>

1 راجع في ذلك : د/ وجدي راغب ، مذكرات في مبادئ القضاء المدني، 1976، بدون دار نشر ، ص45.

الأمر الذي يعكس عدد من المبادئ الإجرائية من ناحية و يبرز كيفية تطوير إجراءات التقاضي والتحول بها إلي الرقمية من ناحية أخرى.

والخصومة هي مجموعة من الإجراءات المتتالية والمرتبطة ببعضها البعض بالتالي فإن الخلل أو العوار الذي من الممكن أن يصيب أي إجراء من شأنه أن يؤثر علي الخصومة بأكملها، فتلك الإجراءات وان تمتعت بالشكلية والدقة يجب مراعاتها علي النحو الذي يقره القانون إلا أن ذلك "ليس غاية لذاته وإنما يبتغي تحقيق ضمانات معينة، وكلها ضمانات لحسن أداء العمل القضائي علي نحو يجعل من ذلك النظام وتلك الشكلية وسيلة لتحقيق الضمانات القضائية¹.

والضمانات القضائية يحققها مجموعة من المبادئ الإجرائية وصولاً إلي تحقيق عدالة المحاكمة بالإعلان مثلاً يتغيا تحقيق مبدأ المواجهة بين الخصوم، وقبل ذلك المطالبة القضائية التي تعد وسيلة لتفعيل الحق في اللجوء إلي القضاء، فعند تطوير آلية الإيداع واستخدام الوسائط الرقمية التي من شأنها أن تضمن تيسير الإجراءات والسرعة والدقة في هذا الصدد، لا بد من الوقوف على الآلية التي سيتم بها هذا الإيداع ليس هذا فحسب .

ومصادقية الوسائل التكنولوجية الحديثة في مجال الاتصال عن بُعد تتجلي في الدقة التقنية للنظام المعلوماتي، وما يقدمه من أمن لمستخدميه، وحيث إن إدخال نظم المعلومات والاتصالات إلي نطاق قضاء الدولة مرهون بإجراءات حماية مستندات الدعوي المقامة رقمياً والتي تهدف إلي تقادي تعديل أو تغيير أو تدمير ملفاتها خاصة في مرحلة الإيداع سواء تم ذلك عمداً أو بإهمال في ظل ضمان سرية وخصوصية المعلومات التي يدلي بها الخصوم في قضاياهم، فلا يجب أن تطغى غاية تسريع وتيرة التقاضي أمام قضاء الدولة من خلال هذه الآليات التقنية علي احترام

1 راجع في ذلك : د/ فاطمة عادل سعيد ، التقاضي عبر وسائل التكنولوجيا والاتصال الحديث ، مرجع سابق ، الجزء الأول ، ص 363 وما بعدها .

المبادئ الأساسية للتقاضي، والتي لا يخرج عنها عدم إفساء أسرار المتقاضين أو التعرض لها من قبل الغير .

مشكلة البحث :

الأصل بالنسبة لرفع الدعوي أن يتم رفعها بواسطة ورقة تسمى صحيفة افتتاح الدعوي أو عريضة الدعوي، وهذه الورقة تودع قلم كتاب المحكمة المختصة بعد أن يتم استيفاء جميع بياناتها وفقا لنص المادة (63) من قانون المرافعات المدنية والتجارية . أما رقميا تعتبر الدعوي مرفوعة إلي المحكمة بناء علي قيام المدعي بمليء الطلب المعد لذلك والموجود علي الموقع الرقمي للمحكمة (الصحيفة الرقمية) ، وهو الأمر الذي يتطلب ضرورة معرفة الآلية التي سيتم بها الإيداع الرقمي لصحيفة الدعوي ؟؟؟ ، و الكيفية التي يتم بها إجراءات المطالبة القضائية عبر الوسائط الرقمية ؟؟؟؟ ، وكذلك معرفة ماهي الآثار المترتبة على المطالبة القضائية ؟؟؟ ، وجميع ما سبق لابد ان يتم فى ظل أمن معلوماتى فكيف سيكون ذلك ؟؟؟؟ ، وما هو موقف النظم القضائية المقارنة ؟؟؟

منهج البحث :

سوف نستخدم المنهج الوصفى بطريقته العلمية الإستوائية والتحليلية لمعالجة النقاط الهامة التي يثرها موضوع الكتاب .

خطة البحث :

هذا وسوف نتناول في هذا الكتاب معالجة موضوع الإيداع الرقمي و أمن المعلومات في ظل التناهي عبر الوسائط الرقمية بالخصومة القضائية على مستوى مبحثين علي النحو التالي :

المبحث الأول : الإيداع الرقمي

المطلب الأول: ماهية الإيداع الرقمي بالخصومة القضائية

المطلب الثاني: إجراءات المطالبة القضائية عبر الوسائط الرقمية

المطلب الثالث: آثار المطالبة القضائية

المطلب الرابع : موقف النظم القضائية المقارنة

المبحث الثاني : أمن المعلومات

المطلب الأول: معايير أمن المعلومات وسلامة البيانات

المطلب الثاني : المخاطر التي تواجه الحق في الخصوصية في بيئة الإنترنت

المطلب الثالث: التحديات التي تواجه أنظمة أمن المعلومات واستراتيجياتها والحماية القانونية

المطلب الرابع :موقف النظم القضائية المقارنة

المبحث الاول

الإيداع الرقمي

للقوف على آلية الإيداع الرقمي واستخدام الوسائط الرقمية التي من شأنها أن تضمن

تيسير الإجراءات والسرعة والدقة في هذا الصدد سنعرض لاحقاً لما يلي :

المطلب الأول: ماهية الإيداع الرقمي بالخصومة القضائية

المطلب الثاني: إجراءات المطالبة القضائية عبر الوسائط الرقمية

المطلب الثالث: آثار المطالبة القضائية

المطلب الرابع : موقف النظم القضائية المقارنة

المطلب الأول

ماهية الإيداع الرقمي بالخصومة القضائية¹

يعني نظام الإيداع الرقمي² لصحيفة الدعوي حق المدعي أو محاميه في تقديم صحيفة الدعوي المتضمنة لطلباته الجوهرية ، والمستندات التي تدعمها إلي المحكمة المختصة³ قانونا عبر موقعها الرقمي علي شبكة الإنترنت⁴ بدلا من تقديمها علي دعائم ورقية لقلم الكتاب الذي يتولى قيدها في السجل المعد لذلك⁵ طبقا لقانون المرافعات المصري، والتي تقضي ب (يقيد قلم الكتاب

1 راجع في ذلك : د/ محمود مختار ، بحث منشور بعنوان "الإيداع الإلكتروني" ، مؤتمر القانون والتكنولوجيا ،كلية الحقوق ، جامعة عين شمس ، ديسمبر 2017. ، الجزء الأول ، ص 465 ، وراجع أيضا : د/ فاطمة عادل سعيد ، التقاضي عبر وسائل التكنولوجيا والاتصال الحديث ، مرجع سابق ، الجزء الأول ، ص 383 وما بعدها

2 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 بالإيداع الإلكتروني انه: { وسيلة إقامة وقيد صحيفة الدعوي وكذا الطلبات العارضة والإدخال والتدخل والتوقيع علي صحفها توقيعيا الكترونيا معتمدا وإيداع المستندات والمذكرات والتي تتم عبر الموقع المخصص لذلك بالمحكمة الاقتصادية المختصة. وهو ما يمكن القياس عليه والاستئناس به في مجال إجراءات التقاضي الإلكتروني أمام القضاء المدني . }

3 راجع في ذلك :

– الإيداع الإلكتروني :

– <https://docplayer.net/18491695-In-the-superior-court-of-fulton-c-state-of-georgia-amended-order-il-1plelventing-electronic-filing-for-civil-cases.html> تاريخ آخر دخول علي الموقع (2020/9/22)

– معايير الإيداع الإلكتروني :

– <https://docplayer.net/11178091-Electronic-filing-standards-implementing-e-filing-program-fourth-judicial-circuit-marion-county-general.html> تاريخ آخر دخول علي الموقع (2020/9/22)

4 راجع في ذلك :

– Fabien GELINAS، Interopérabilité et normalisation des systèmes de cyber، justice : *Orientations*، p 2، www.lex-electronica.org/docs/articles_62.pdf

5 راجع في ذلك : د/ علي بركات ، الوجيز في شرح قانون المرافعات المدنية والتجارية ، دار النهضة العربية ، 2012، ص 427 ، وما بعدها .

الدعوي / عملاً بحكم المادة (٦٧) في يوم تقديم الصحيفة في السجل الخاص بذلك بعد أن يثبت في حضور المدعي أو من يمثله تاريخ الجلسة المحددة لنظرها في أصل الصحيفة وصورها (.....). وعرفها أحد الفقهاء الفرنسيين بأنها (تلك الخدمة القضائية المميكنة، والتي يعتمد محامي الخصم عليها لإجراء حوار رقمي مع المحكمة المختصة عبر موقعها الرقمي علي شبكة الإنترنت لتقديم صحيفة الدعوي والطلبات ومذكرات الدفاع والدفع والمستندات وغيرها من الأوراق القضائية، وذلك علي مدار اليوم كاملاً ودون التقيد بمواعيد العمل الرسمية)¹ ويترتب علي الأخذ بهذه الآلية الرقمية في مجال التقاضي العادي الآتي:

١ الحد من تداول المستندات الورقية أمام المحاكم، وتقليل تنقل الخصوم و محاميتهم لمقر هيئة المحكمة لتقديم أوراق قضائهم . كما يستطيع المحامي - عبر هذه التقنية الفنية - القيام بأكثر من إجراء قضائي في وقت وجيز، مثل إرسال المستندات والأوراق إلي قلم الكتاب الرقمي، ودفع رسوم الدعوي بواسطة وسائل الدفع الرقمي².

٢ الحد من الآثار السلبية الناجمة عن تداول المستندات الورقية بين المحكمة والخصوم مثل فقدان ملف الدعوي، أو عدم استحضار ملف الدعوي سريعاً، والحاجة إلي مكان واسع لتخزين هذه الوثائق الورقية (الأرشيف) وهو ما سينحصر في حالة الحفظ الرقمي للأوراق والمستندات في ذاكرة الحاسب الآلي للمحكمة.

1 راجع في ذلك :

- Caroline BOISSEL، e-greffe : de la dématérialisation des actes de procédure vers le développement d'une justice en ligne ؟، mémoire، 2004 ؛
www.memoireonline.com /.../m_utilisation-nouvelles-technologies-، p.4

2 راجع في ذلك : د/ محمد صابر احمد، " دور الحاسب الآلي في تيسير إجراءات التقاضي " ، مرجع سابق ، ص42 وما بعدها.

وفي حالة اللجوء إلي التقاضي عبر الوسائط الرقمية، من الضروري إيجاد حل يضمن الأمن الرقمي للإيداع ، وتري الباحثة إنه من الممكن أن تقوم وزارة العدل المصرية بتكليف شركة تعمل في مجال أمن البيانات او الأمن المعلوماتي بتبني حماية كافة البيانات والمستندات الخاصة بالدعوي الرقمية وذلك علي مستوي كافة المراحل التي تمر بها الدعوي الرقمية وهو ما يطلق عليه إجراءات حماية مستندات الدعوي المقامة رقميا¹ ، وهو مجال سيوفر الكثير من الفرص الاستثمارية في القطاع العام أو القطاع الخاص . وبالتالي يتحقق العلم اليقيني في مجال الإيداع الرقمي تضمنه الشركة المسؤولة عن امن وحماية البيانات أو الشركة التي ستتولي عملية إعلان وإرسال الملفات من جانب المحكمة إلي المتقاضين².

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 بطرق حماية إقامة وسير الدعوي الكترونيا بانه : { إجراءات حماية مستندات الدعوي المقامة الكترونيا والتي تهدف إلي تقادي تعديل أو تغيير أو تدمير ملفاتهما سواء تم ذلك عمدا أو بإهمال . وهو ما يمكن الاستئناس به لتحديد ماهية امن وسلامة المعلومات بالتقاضي الإلكتروني بالقضاء المدني } .

2 تجدر الإشارة هنا الي انه سوف تقع علي الشركة التي ستتبني القيام بالتبليغ أو الإعلان الإلكتروني ، سواء كانت شركة اتصالات كشركة فودافون مثلا أم شركة مسؤولة عن برامج الكمبيوتر ك google سوف تتحمل المسؤولية الكاملة عن إعلام الشخص والتحقق من وصول الإعلان واستلامه إليه بشخصه وهو ما يمكن أن يتم باستخدام الرقم القومي للشخص والتوقيع الرقمي علي جميع ملفات الدعوي عند إيداع أو استلام أي ملف أو إعلان ، و أيضا الشركة التي سوف تتحمل مسؤولية حماية وتأمين البيانات الخاصة بالدعوي الإلكترونية علي مستوي جميع مراحل الدعوي . وتري الباحثة انه من الممكن في ذلك الاستئناس بم نص عليه قانون 175 لسنة 2018 الخاص بالجرائم الإلكترونية بالمادة (2) التزامات وواجبات مقدم الخدمة.

المطلب الثاني

إجراءات المطالبة القضائية عبر الوسائط الرقمية¹

حاولت النظم القضائية المختلفة البحث عن حل لمشكلة تأخر البت في الدعاوي نتيجة لتكدس المحاكم بالقضايا ، و كان من الضروري علي هذه النظم القضائية أن تبحث عن الآليات التي من شأنها أن تؤدي إلي تيسير ولوج المتقاضي لباب القضاء ، بإضفاء طابع المرونة علي الإجراءات القضائية، وتبسط قواعد العمل القضائي، ورفع مستوى الاتصال بين جهات القضاء من ناحية والخصوم ووكلائهم من ناحية أخرى، وترشيد نفقات التقاضي علي جمهور المتقاضين. وهو ما أدى إلي زيادة أهمية استخدام النظم القضائية لتكنولوجيا² المعلومات والاتصالات كمحاولة للاستفادة من خصائص التقنيات الحديثة - كسرعة ودقة الأداء لتيسير العمل القضائي وتبسيط إجراءاته علي جمهور المتقاضين تحقيقا للفصل في قضاياهم علي وجه السرعة ، وهو ما يتلاقى مع إرادة كافة الدول في إدخال التكنولوجيا لمجال التقاضي والتحول الي الرقمية³. فلا يخفي أن الاتجاه العام لجميع دول العالم الآن نحو الاستفادة من تقنية المعلومات في تسيير

1 راجع في ذلك كلا من:

- د / إبراهيم محمد السعدي ، دور التكنولوجيا في التغلب علي ظاهرة البطء في التقاضي، دور التكنولوجيا في التغلب على ظاهرة البطء في التقاضي امام القضاء المدني في مصر، مؤتمر القانون والتكنولوجيا ،كلية الحقوق، جامعة عين شمس ، ديسمبر 2017 ، الجزء الأول ، ص 505 وما بعدها .
- د/ فاطمة عادل سعيد ، التقاضي عبر وسائل التكنولوجيا والاتصال الحديث ، مرجع سابق ، الجزء الأول ، ص 380 وما بعدها .

2 راجع في ذلك :

Timothy J. Chorvat and Laura E. Pelanek , Electronically Stored Information in Litigation Source, The Business Lawyer , November 2010, Vol. 66, No. 1 (November 2010), p 183- 189 , Published by: American Bar Association Stable , , URL: <https://www.jstor.org/stable/25758532>

3 راجع في ذلك : د/ قدرى محمد محمد مصطفى محمود ، حماية المستهلك في العقد الإلكتروني ، رسالة ماجستير ، جامعة القاهرة ، 2012 ، ص 5 .

الأعمال العامة وتبسيطها علي جمهور المواطنين خاصة في ظل الكوارث والأزمات والأوبئة كوفيد 19 - والذي أضطر معه العالم أجمع الي التحول الي الرقمية في شتي مجالات وأنشطة البشر علي كوكب الأرض والتي كان من أهمها التحول الي الرقمية في مجال التقاضي . فالحكومة الرقمية موجودة الآن وبقوة بالعديد من الدول العربية² ، أما بالنسبة للدول الغربية فنجد سويسرا سبقت بها ضمن مشروع قانون القاضي الرقمي والذي بدأ منذ عام ٢٠٠١ والخاص بتحديث النظام المعلوماتي للسلطة القضائية ضمن سلسلة من المشروعات المعلوماتية للنهوض بأداء السلطات العامة في الدولة لخدماتها العمومية، والتي لا تخرج عنها الخدمات المقدمة من السلطة القضائية ، وفي نطاق القضاء السنغافوري ، أخذ هذا القضاء بنظام الإجراءات الرقمية³ والذي يعد طليعة النظم التكنولوجية القابلة للتطبيق في النظم القضائية المختلفة، والذي يستند إلي إدخال التكنولوجيا الحديثة لتسيير العمل القضائي بشكل عام . وما قامت به النظم القضائية السابقة يؤكد علي مواكبة أليات العمل القضائي للمتغيرات التكنولوجية التي ترد علي المجتمع تطبيقا لضرورة المراجعة الحقيقية لطرق مباشرة الخصوم للإجراءات المدنية، وليس مجرد المراجعة الشكلية أو السطحية فقط⁴.

1 Civil Litigation in the time of Covid-19: Everything you need to know and consider
www.2tg.co.uk

2 راجع في ذلك : د/ محمد المتولي : تأهيل الكوادر البشرية لتطبيق الحكومة الإلكترونية في الدول العربية ، ص 1 وما بعدها ، بحث منشور علي موقع منتدي الحكومة الإلكترونية الإسلامية .

– www.e-govs.com

3 راجع في ذلك : محمود مختار، استخدام تكنولوجيا المعلومات لتسيير إجراءات التقاضي المدني ، دراسة مقارنة ، دار النهضة العربية ، ط ٢٠١٣ ، ص ٣٣ .

4- Refer to that:

- <https://file.supremecourt.gov>
- www.elitigation.sg
- www.clio.com
- www.classic.austlii.edu.au
- www.supremecourt.gov.sg،
- www.netfind.com

ويعد اعتماد طريقة رقمية لرفع الدعوي أمام القضاء خطوة أساسية علي طريق تطوير نظام رقمي كامل للتعامل مع ملفات المحكمة ولكن ذلك يواجه عدد من التحديات الأساسية علي النحو التالي¹:

١. كيف يمكن ان يتأقلم المتقاضين مع النظام الرقمي : في الوقت الحالي لم تعد التكنولوجيا ولا كيفية استخدامها بالأمر الصعب، علي العكس من ذلك فإنه متاح للكافة وازداد توافر وسائل الاتصال بوجود الهواتف الذكية واتصالها بالإنترنت الأمر الذي من شأنه أن يجعل الوصول إلي موقع المحكمة ورفع الدعوي أمر في غاية السهولة، ومع ذلك فعلي فرض وجود شريحة من المتعاملين مع مرفق القضاء لا يمكنهم استعمال هذه الوسائل فإنه يمكن أن تلحق بالمحكمة مكاتب (المساعدة القضائية) بها أجهزة للحاسب الآلي وموظفين مختصين بإمكانهم مساعدة المتقاضين في رفع الدعوي رقميا ، ورغم إنه قد يبدو أن الذهاب للمكاتب الملحقة يفوت هدف السرعة وتوفير الوقت والجهد لأنه سيكون علي المتقاضين الذهاب بأنفسهم إلي المحكمة إلا أن هذا الأمر سوف يتم علي مستوي المرحلة الأولى فقط من التحول لرقمية الإجراءات . كما أن ذلك سيعتبر مساهمة في هدف أكبر وهو حفظ كافة القضايا وملفات المحكمة رقميا.

- <http://bo-ecli.eu/ecli/european-e-justice-portal>،
- https://e-justice.europa.eu/content_european_case_law_identifer_ecli-175-en.do
- <http://www.alittihad.ae/details.php?id=52871&y=2016&article=full> ،
- <http://www.singaporelaw.sg/sglaw/laws-of-singapore/overview/chapter-2> --
- <http://braddellbrothers.com/litigation.html>.-

1 راجع في ذلك : د/ فاطمة عادل سعيد ، التقاضي عبر وسائل التكنولوجيا والاتصال الحديث ، مرجع سابق، الجزء الأول ، ص380 وما بعدها ، وراجع أيضا:

- Sophia BINET، L'utilisation des nouvelles technologies dans le procès civil : Vers une procédure civile intégralement informatisée.p72 .

٢. حماية ملفات القضايا والسرية بالنسبة للمتقاضين¹ : إن وجود ملفات القضايا وإتاحتها

للاطلاع للكافة قد يؤدي إلي نتائج بالغة الخطورة بالنسبة للمتقاضين و لكننا نري أن هذا الأمر لا يعد العقبة في طريق اعتماد نظام رقمي لتسيير إجراءات الدعوي، ففي ألمانيا علي سبيل المثال ملفات المحكمة غير متاحة للكافة بل للمتقاضين أطراف القضية ومن يمثلهم فقط فلا يمكن لأي من كان الدخول إليها.

فضلا عن السرية وسهولة أو صعوبة التعامل مع التكنولوجيا ، فإننا نؤيد أن الصعوبة الحقيقة التي تواجه فكرة رفع الدعوي رقميا هي العدالة الإجرائية فعلي الرغم من النظام الجامد الذي تحتته الشكلية ومن ذلك ضرورة تطلب الوريقات إلا إنها تضمن التأكد من وصول الإعلان والعلم بالقضية في جانب المدعي عليه وما يستتبعه من ممارسة حقه في الدفاع وهو ما يفترض معه مرور فترة زمنية معينة فهل سيكون لدي المدعي أجلا لتحضير دفاعه علي فرض الأخذ برقمية التقاضي أم إنه من الممكن أن يؤدي ذلك إلي إهدار ضمانات التقاضي خاصة أن الأسبقية في هذا الفرض ستكون للمدعي علي اعتبار إنه رافع الدعوي.

وتري الباحثة في ذلك إنه لكي تتحقق العدالة الإجرائية في التقاضي الرقمي² يجب أن

يتوافر عدة نقاط كلها علي نفس الدرجة من الأهمية :

1Refer to that:

Kirley, Elizabeth Anne, "Reputational Privacy and the Internet: A Matter for Law?" (2015). PhD Dissertations.p 8. <http://digitalcommons.osgoode.yorku.ca/phd/8> (تاريخ آخر دخول علي الموقع : 2021/1/8)

2 راجع في ذلك :

– قوانين التكنولوجيا وتكنولوجيا القانون :

– Daniel B. Garrie, & Daniel K. Gelb, An Argument for Uniform E-Discovery Practice in Cross-Border Civil Litigation, 7 J. Bus. & Tech. L. p341-359 (2012) Available at: <http://digitalcommons.law.umaryland.edu/jbtl/vol7/iss2/4>

➤ لابد من متابعة رئيس المحكمة لإدارة الدعوي رقميا من جانب القضاة ، علي أن يراقب القاضي عملية الإيداع¹ بقلم الكتاب الرقمي والإعلان الرقمي لأوراق الدعوي ومحاسبة كل من يقصر أو يخل بنظام التقاضي الرقمي كلا حسب مسؤوليته وموقعه ، كما أن القاضي هو المسئول عن إدارة الجلسة والتي سوف تتم بالوسائط الرقمية .

➤ يجب ان يتم جميع ما سبق ذكره تحت رقابة هيئة يتم إنشاءها داخل وزارة العدل " تحت مسمي هيئة الرقابة الرقمية و التفتيش الرقمي " بها قضاة وخبراء وفنين يقفون علي آخر تطورات تكنولوجيا المعلومات والبيئة الرقمية . للرقابة علي القاضي المسئول عن إدارة الدعوي الرقمية فنيا .

➤ لضمان موثوقية وأمان الدليل الرقمي يجب الرجوع لهيئة صناعة تكنولوجيا المعلومات لإضفاء الحجية علي الدليل الرقمي . كما ترى الباحثة إنه يجب إنشاء أكثر من هيئة

– https://www.researchgate.net/publication/251341160_The_Laws_of_Technology_and_the_Technology_of_Law (تاريخ آخر دخول علي الموقع 2020/9/22)

اراجع في ذلك :

– تعليمات المستخدم في نظام الإيداع الإلكتروني :

– <https://docplayer.net/16506977-User-instructions-welcome-to-the-clerk-s-office-electronic-filing-system.html> (تاريخ آخر دخول علي الموقع 2020/9/22)

– تأمين ودمج عمليات نقل الملفات عبر الإنترنت :

– <https://docplayer.net/15798654-White-paper-securing-and-integrating-file-transfers-over-the-internet.html> (تاريخ آخر دخول علي الموقع 2020/9/22)

– الإيداع الإلكتروني في محكمة الاستئناف :

– <https://docplayer.net/11178265-St-bernard-parish-electronic-filing-at-the-louisiana-court-of-appeal-fourth-circuit-by-judge-roland-belsome-judge-daniel-dysart-and-dennis.html> (تاريخ آخر دخول علي الموقع 2020/9/22)

– إرشادات نظام الإيداع الإلكتروني :

– <https://docplayer.net/15293838-The-workers-compensation-court-s-electronic-filing-system-guidelines.html> (تاريخ آخر دخول علي الموقع 2020/9/22)

لضمان ومراقبة المعاملات في البيئة الرقمية¹ ، وما ينتج عنها من أدلة ومستندات

رقمية يجب التحقق من حجيتها .

وفي هذا المجال سوف نعرض لاحقاً إلى :

الفرع الأول : كيفية إجراء المطالبة القضائية

الفرع الثاني : جزاء النقص أو الخطأ في البيانات المقدمة بطلب عرض النزاع

1 راجع في ذلك : [الحكم رقم 16 - لسنة 2015 - تاريخ الجلسة 29 / 9 / 2015] المحاكم الاقتصادية.

الفرع الأول

كيفية إجراء المطالبة القضائية¹

ترتبط المطالبة القضائية بما يقرره كل نظام للإجراءات المدنية في كل دولة وما يضيفه عليه من شكلية وبداية من ذلك يمكن تحديد مدى الاستخدام الملائم للتكنولوجيا لإتمام هذا الإجراء.

والأصل العام بالنسبة لرفع الدعوي الورقية وفقا لنص المادة (63) من قانون المرافعات أن يتم رفعها بواسطة ورقة تسمى صحيفة افتتاح الدعوي أو عريضة الدعوي، وهذه الورقة تودع قلم كتاب المحكمة المختصة بعد أن يتم استيفاء جميع بياناتها وتوقيعها من محام مقبول للترافع أمام المحكمة التي يتم إيداع قلم كتابها هذه الصحيفة، وذلك كله ما لم ينص القانون علي غير ذلك من إجراءات ترفع بها الدعوي.

أما رقميا تعتبر الدعوي مرفوعة إلي المحكمة بناء علي قيام المدعي بمليء الطلب المعد لذلك والموجود علي الموقع الرقمي للمحكمة (الصحيفة الرقمية)²، وتودع قلم الكتاب رقميا الإجراءات ما لم ينص القانون علي غير ذلك.

1 راجع التفاصيل التقنية لإجراء المطالبة القضائية إلكترونيا ، الباحث د/ محمد صابر احمد ، " دور الحاسب الآلي في تيسير إجراءات التقاضي " ، مرجع سابق ، ص97 وما بعدها ، وقد آثرنا الإشارة دون الإفاضة لعدم اتساع المجال لذلك.

2 راجع في ذلك :

– Courtroom Technology:

Moyeda، Jessica، "Courtroom Technology" (2014)، Cornell Law School Graduate Student Papers ، Paper 30. http://scholarship.law.cornell.edu/lps_papers/30 (تاريخ

(آخر دخول علي الموقع : 2021/1/8)

وفي هذا الصدد يتعين التفرقة بين إيداع صحيفة الدعوي وإعلانها ، ذلك إنه ، وعلي حسب ما جري عليه قضاء النقض ، إيداع الصحيفة قلم الكتاب ضد الخصم المعني بالخصومة يعتبر إجراء لازم لإجراء المطالبة القضائية ، أما إعلان صحيفة الدعوي فهو إجراء لازم لانعقاد الخصومة بين طرفيها ، وبالتالي لا يغني إيداع الصحيفة قلم كتاب المحكمة المختصة عن وجوب إعلان الخصوم بها¹.

وفي هذا الشأن قضت محكمة النقض " بأن مفاد نص المادتين ١ / ٩٣ ، 94 مرافعات إنه وأن كان يلزم لإجراء المطالبة القضائية إيداع صحيفة الاستئناف قلم كتاب المحكمة وهو ما يترتب عليه ، كأثر إجرائي ، بدء الخصومة ، إلا أن إعلان صحيفة الاستئناف إلي المستأنف عليه الاستئناف يبقي إجراء لازما لانعقاد الخصومة بين طرفيها ويكون وجودها الذي بدأ بإيداع صحيفة تخلف قلم الكتاب معلقا علي شرط إعلانها إلي المستأنف عليه إعلان صحيحا ، فان هذا الشرط حتي صدور الحكم الاستئنافي زالت الخصومة كأثر للمطالبة القضائية ، ومن ثم تبطل الخصومة التي لم تعلن صحيفتها هي وجميع الأحكام التي تصدر فيها ، فيقع باطلا الحكم الصادر علي من لم يعلن إطلاقا بصحيفة الاستئناف² .

وباستخدام مواقع الويب يستطيع المتقاضين والمحامين الدخول علي الموقع المحكمة المختص والاطلاع علي الفيديو الخاص بطريقة رفع الدعوي خطوة بخطوة أو تحميل الملف الخاص بشرح إجراءات التقاضي الرقمية كما يمكنهم تحميل كافة صيغ الدعاوي التي تلزمهم أو ملئ النماذج الموجودة علي موقع المحكمة . وبعد ذلك يتم إرفاق **attach** أي ملفات إضافية

– Electronic Technology and Civil Procedure New Paths to Justice from Around the World : Miklós Kengyel ، Zoltán Nemessányi، p101(: الموقع علي الموقع : 2021/1/8) .

1 راجع في ذلك : أ.د/ الأنصاري حسن النيداني، قانون المرافعات المدنية والتجارية ، بدون سنة نشر ، ص 137.

2 الطعن رقم ٧٩١ لسنة 40 ق - جلسة ١٩٧٩ .

يحتاج أن ترفق إلي صحيفة الدعوي ، ويتم وضع هذه المستندات والملحقات في سجل بيانات رقمي **Electronic Data Envelope** ، وهذا السجل تصممه المحكمة خصيصا لنظام التقاضي الرقمي ويمكن تعديله وتحديثه لمواجهة متطلبات التقاضي عبر الوسائط الرقمية وإذا كانت هناك دعاوى فرعية مرتبطة يتم ربطها بالدعوي الأصلية ويقوم نظام المعالجة بتقسيمها إلي مجموعات حيث ترسل كل مجموعة إلي المحكمة المختصة ، سواء كانت المحكمة الجزئية أم الابتدائية أم الاستئناف أم النقض ، ويتم ذلك من خلال الإدارة الرقمية للعدالة بكافة مراحل الدعوي بالتقاضي الرقمي .

وعند وصول صحيفة الدعوي والمستندات إلي موقع المحكمة المختصة يقوم الموظف المختص بفحص الصحيفة والمستندات ويقرر قبولها أو عدم قبولها ، وفي الحالتين يرسل رسالة بالبريد الرقمي إلي المتقاضي أو المحامي يفيد به بالقبول أما في حالة عدم القبول فإن الموظف يحدد له سبب ذلك ويبين له الأجراء الصحيح الواجب الإلتباع لقبول المستندات مرة أخرى ، ومن أمثلة عدم قبول الصحيفة ، عدم سداد الرسوم القضائية أو سداد جزء منها فقط ، أو عدم توقيع محام علي الصحيفة ويقصد بالطبع هنا التوقيع الرقمي وليس التوقيع اليدوي ، أو أن تكون الصحيفة محتوية علي بيانات مخالفة للنظام العام والآداب. و بمجرد إرسال المستندات رقميا يتم تحويلها إلي كل من موقع الخادم **Server** الخاص بالمحكمة المختصة وموقع الخادم الخاص بالشركة القائمة علي تنفيذ عملية نقل المستندات ، حيث يقوم قلم كتاب المحكمة باعتماد تلك الأوراق في ذات اليوم والوقت .

الغصن الأول

البيانات الواجب توافرها في الطلب المقدم عبر إجراءات التقاضي الرقمي

ويجب أن تشمل صحيفة الدعوى الرقمية¹ علي البيانات الآتية :

البيان الأول: المدعي:

ويجب أن يشتمل بيان المدعي علي عدة حقول، الحقل الأول يحتوي علي اسم المدعي وفيه يجب توضيح الاسم الأول للمدعي واسم الأب والجد واللقب أي أن يكون الاسم رباعياً، والحقل الثاني يشتمل علي بيان مهنته أو وظيفته وعنوان عمله إن تيسر ذلك، والحقل الثالث يشتمل علي بيان موطن المدعي، والرابع يشتمل علي بيان الرقم القومي، والخامس يشتمل علي البريد الرقمي الحكومي للمدعي والذي سيتم تطبيقه مع بداية العمل بنظام التقاضي الرقمي، حيث يجب أن يتم إنشاء بريد رقمي حكومي لكل فرد في الدولة يحمل بطاقة رقم قومي يكون خاص به والذي سيتم عن طريقه مخاطبته بجميع المراسلات الحكومية الرسمية، أما عن الحقل السادس فيشتمل علي رقم الهاتف الخليوي للمدعي والفائدة من هذا البيان إنه سيتم إرسال إشعار في صورة رسالة نصية للمتقاضي بأنه توجد مراسلات من المحكمة علي بريده الرقمي، وإن لم يكن هناك هاتف خلوي للمدعي فيتم كتابة رقم الهاتف الأرضي له وسيتم إرسال الإشعار السالف ذكره في صورة برقية عن طريق الشركة المصرية للاتصالات علي عنوانه على ان يضاف إلى صحيفة الدعوى تعهد من جانب صاحب البيانات بالتزامه بأنه في حالة تغيير أى بيان من البيانات السابقة فإنه ملتزم بإبلاغ المحكمة .

1 راجع في ذلك : د/ أحمد محمد عبدالرحمن ، نظرة حول نظام التقاضي الإلكتروني في مصر، بحث مقدم للمؤتمر العلمي الحادي عشر "الاتجاهات الحديثة في القانون الإجرائي" ، كلية الحقوق ،جامعة أسيوط ، مارس

البيان الثاني: المدعي عليه:

ويجب أن يشتمل بيان المدعي عليه علي ذات البيانات الخاصة بالمدعي إن تيسر ذلك إلا أن هناك حقول بدون ملئها لن يتم قبول الطلب كالحقل الخاص باسم المدعي عليه علي أن يتم ملئ الثلاثة حقول الأولي علي الأقل الخاصة بالاسم الأول واسم الأب واسم الجد أو اللقب، ويجب أيضا ملئ الحقل الخاص بالمهنة أو الوظيفة، وكذلك يجب ملئ الحقل الخاص بموطن المدعي عليه، وإن تيسر للمدعي معرفة البريد الرقمي الحكومي الخاص بالمدعي عليه فيتم كتابته، ويتم كتابة رقم هاتف المدعي عليه الخلوي أو الأرضي، وذلك للتيسير علي الموظف المختص لتمكينه من معرفة البريد الرقمي الخاص بالمدعي عليه حتي يتم إرسال إشعار له.

البيان الثالث: المحكمة المرفوعة أمامها الدعوي:

وهي المحكمة المختصة بنظر هذا الطلب، وهذا الحقل تتسدل منه قائمة نوع المحكمة جزئية أو ابتدائية أو استئناف أو نقض وإذا كانت إحدي الثلاث الأولي فيتم النقر علي احدها وبعدها تتسدل قائمة آخري توضح المحافظة التي توجد بها المحكمة المراد نظر هذا الطلب أمامها وتحديد المدينة إذا كانت جزئية بعد تحديد المحافظة¹.

البيان الرابع: وقائع الدعوي:

وهي المعلومات المتعلقة بالنزاع وظروف نشأته بالتفصيل الممكن وحسب التاريخ والسبب الذي تؤسس عليه الدعوي، والغرض من هذا البيان هو تمكين المدعي عليه من العلم بالادعاء الموجه ضده حتي يستعد للدفاع عن نفسه، كما إنه يعين المحكمة علي تكوين فكرة واضحة عن موضوع الدعوي.

1 راجع في ذلك : د/ أحمد محمد عبدالرحمن ، نظرة حول نظام التقاضي الإلكتروني في مصر، مرجع سابق ،

البيان الخامس: الطلبات المتعلقة بحسم النزاع وأسانيد هذه الطلبات:

وبالنسبة للبيانين الأخيرين يمكن عدم ملئهما والاستغناء عنهما بأن يتم كتابة عريضة الدعوي كاملة كما في الدعوي الورقية أي في نفس الشكل والقالب ويتم تحويلها إلي صيغة PDF وذلك حتي لا يتم التلاعب فيها بالزيادة أو الحذف ويتم رفعها إلي الموقع عن طريق وجود أيقونة تجيز لمقدم الطلب أن يقوم بمليء فراغات البيانين الرابع والخامس أو أن يقوم برفع عريضة الدعوي المحولة إلي صيغة PDF إلي موقع نظام التقاضي الرقمي¹ الخاص بالمحكمة .

البيان السادس: بيان موطن مختار للمدعي:

حيث يقوم المدعي بتحديد موطن مختار له في البلدة التي بها مقر المحكمة المرفوع أمامها الدعوي إن لم يكن له موطن فيها، وهذا البيان ليس جوهريا علي الإطلاق حيث إنه لا يترتب علي إغفاله أي جزء، حيث إنه يجوز للخصوم إعلانه بأوراق الدعوي في قلم الكتاب². وتري الباحثة إنه في ظل رقمية إجراءات التقاضي لا فائدة من هذا البيان حيث إنه كما سنذكر لاحقا أن إعلان جميع الأوراق القضائية سيتم إعلانها برسائل رقمية دون الوسائل الورقية المتبعة حاليا، وبالتالي فإنه لن تكون هناك مشقة من إعلان المدعي أو المدعي عليه في أي مكان كان حتي ولو كانت إقامته بالخارج أي خارج البلاد في أي دولة آخري أيا كانت وأيا كان بعد المسافة.

1 راجع في ذلك كلام من :

- www.e-filling.com، www.maillycy.fr
- www.moj.gov.sa

2 راجع في ذلك : أ.د/ الأنصاري حسن النيداني ، قانون المرافعات المدنية والتجارية ، مرجع سابق ، ص 135.

الفصل الثاني

المتطلبات الآخري لقبول طلب رفع الدعوي رقميا

ويقوم قلم كتاب المحكمة عبر الوسائط الرقمية بقيد صحيفة الدعوي بشرط أن تستوفي ما

يلي:

١ - ما يدل علي سداد الرسوم المقررة قانوناً أو ما يفيد الإعفاء منها.

٢ - إرفاق المستندات المؤيدة للدعوي تحت مسؤولية المدعي وما يركن إليه من أدلة

لإثبات دعواه.

٣ - مذكرة شارحة للدعوي.

وهو ما سنعرض له علي النحو التالي :

➤ سداد الرسوم المقررة قانوناً¹:

حيث إنه وفقاً لنص المادة (14) من قانون الرسوم القضائية فإن الدولة تفرض رسوماً

قضائية عند رفع دعاوي يلتزم المدعي بسدادها سواء كانت رسوم أصلية وتتمثل في الرسم

النسبي والثابت المقرر أو رسوم تكميلية وتتمثل في رسم صندوق الخدمات الصحية والاجتماعية

أو رسم إضافي لصندوقه أبنية المحاكم.

ويمكن سداد تلك الرسوم رقمياً وذلك بالوسيلة التي توفرها المؤسسات المالية المصرفية

وغير المصرفية لسداد كافة رسوم استخدام خدمة التقاضي الرقمي بالمحكمة المختصة بنظر

الدعوي والرسوم القضائية والدمغات المقررة لإقامة دعاوي ومنها البطاقات المدفوعة مسبقاً "

1 راجع في ذلك :

- أمان للمدفوعات الرقمية :

- <https://www.lawtechnologytoday.org/2020/07/five-safety-tips-for-digital-payments/> (تاريخ آخر دخول علي الموقع 2020/9/22)

بطاقات السحب والائتمان" والحوالات المصرفية ، أو عن طريق سداد تلك الرسوم بواسطة نظام فوري والأخيرة هي شبكة مدفوعات متنوعة تشمل ماكينات الصرف الآلي والمنافذ التجارية بالإضافة للدفع عن طريق الإنترنت.

ووفقا لنص المادة (65) من قانون المرافعات فإنه يجب قبول قيد الدعوي إذا كانت مصحوبة بما يدل علي سداد الرسوم المقررة قانونا أو إعفاء المدعي منها، ويجب في هذا الصدد أن يتم إعطاء المدعي مهلة محددة بنص القانون يتم سداد الرسوم المحددة قانونا خلالها والتي تم إرسال قيمتها للمدعي مسبقا، وتبدأ هذه المهلة من التاريخ الذي يتم فيه إرسال رسالة سواء نصية علي التليفون المحمول الخاص بالمحامي أو المدعي أو البريد الرقمي للمحامي أو المدعي. ويلاحظ في هذا الصدد إنه إذا تم رفع الدعوي دون أداء الرسم المطلوب فإنها لا تنتج أي أثر قانوني، إلا إنه لا تسري آثار رفع الدعوي إلا من تاريخ استكمال الرسم القانوني وعندئذ لا تسري آثار رفع الدعوي إلا من الوقت الذي يستكمل فيه الرسم، فجزاء عدم سداد الرسم ألا يتم نظر الدعوي وألا يتم تحديد جلسة لها منذ البداية، حيث إنه لا يترتب علي سداد الرسم المقرر جزاء البطلان لأن المخالفة المالية بعمل ما لا ينبني عليها بطلان هذا العمل.

➤ إيداع المستندات المؤيدة للدعوي¹ :

والتساؤل هنا يدور حول كيفية تقديم المستندات عند رفع الدعوي رقميا؟²

يمكن الإجابة علي هذا التساؤل بأنه يمكن استخدام جهاز الماسح الضوئي في إدخال صور المستندات إلي الحاسوب حيث يحولها من طبيعتها الرسومية إلي صورة رقمية حتي تلائم

1 راجع في ذلك :

– Electronic Technology and Civil Procedure New Paths to Justice from Around the World، Miklós Kengyel ، Zoltán Nemessányi،p233 .

2 راجع في ذلك : د/ أحمد محمد عبدالرحمن ، "نظرة حول نظام التقاضي الإلكتروني في مصر" ، مرجع سابق، ص15 وما بعدها .

طبيعة الحاسوب وحتى يسهل تخزينها داخل ملف واحد واستدعائها وقت الحاجة إليها، ويمكن بعد ذلك تحويل تلك الصور الرقمية إلي صيغة PDF حتي لا يمكن التلاعب بها وبعد أن يتم ذلك يمكن أن يتم رفع الملف الموجود علي جهاز الحاسوب في صيغة pdf إلي الموقع المخصص للدعوي التي يرفعها المدعي ويجب أن يتم ذلك مع رفع الدعوي.

فإنه إذا لم يقدم المدعي المستندات الدالة علي صحة ادعائه أثناء رفع الدعوي فإنه يجوز له تقديمها بعد ذلك في أية حالة كانت عليها الدعوي حتي قبل إقفال باب المرافعة في الدعوي. ووفقا لنظام الدعوي الرقمية فإنه لا يترتب علي مخالفة تلك القاعدة أي جزاء سواء كان بطلان أو سقوط ، لذلك فإنه إذا لم يقدم المدعي المستندات الدالة علي صحة ادعائه أثناء رفع الدعوي فإنه يجوز له تقديمها بعد ذلك في أية حالة كانت عليها الدعوي حتي قبل إقفال باب المرافعة في الدعوي.

و يمكن تتبع سير الدعوي¹ بداية من طلب رفع الدعوي من المدعي إلي المحكمة المختصة وبالتالي تتعدد الخصومة، علي النحو التالي:

يقوم المدعي بتوكيل محامي للدفاع عنه بشكل رقمي عن طريق الربط الرقمي بين موقع المحكمة وموقع المحامي فيستصدر وكالة بالخصومة بعد إدخال بياناته المطلوبة ، ويتم التأكد من تلك البيانات من خلال الربط الرقمي مع مصلحة الأحوال المدنية ، فيستطيع المحامي إدخال رقمه الكودي الذي يحصل عليه من نقابته في إطار مشروع الحكومة الرقمية ، وتعتبر الدعوي مرفوعة إلي المحكمة بناء علي طلب المدعي بصحيفة رقمية تودع قلم الكتاب رقميا ما لم ينص القانون علي غير ذلك. وعلي قلم الكتاب إثبات تاريخ طلب القيد في جميع الأحوال ، وإذا رأي

[راجع في ذلك : د / إبراهيم محمد السعدي ، دور التكنولوجيا في التغلب علي ظاهرة البطء في التقاضي ، مرجع سابق ، الجزء الأول ، ص 493 وما بعدها .

قلم الكتاب عدم قيد صحيفة الدعوي لعدم استيفاء المستندات والأوراق الموضحة عالية ، قام بعرض الأمر علي قاضي الأمور الوقتية ليفصل فيه فوراً ، إما بتكليف قلم الكتاب بقيد الدعوي أو بتكليف طالب قيدها باستيفاء ما نقص ، وذلك بعد سماع أقواله من خلال الموقع الرقمي والتواصل معه من خلاله ، فإذا قيدت صحيفة الدعوي تنفيذاً لأمر القاضي، اعتبرت مقيدة من تاريخ تقديم طلب القيد ، ويرسل قلم الكتاب إلي المدعي عليه صحيفة الدعوي والمذكرة الشارحة لدعوي المدعي عليه ، ويخطر به قيد الدعوي واسم المدعي وطلباته والجلسة المحددة لنظرها، ويدعوه إلي الاطلاع علي ملف الدعوي وتقديم مستنداته ومذكرة بدفاعه لأنه لا تعتبر الدعوي مرفوعة والخصومة قائمة الا بهذا الإعلان والذي يرتب جميع الآثار الناجمة عن رفع الدعوي من قطع التقادم وسريان الفوائد¹. وعلي المدعي عليه أن يودع رقمياً قلم الكتاب مذكرة بدفاعه ويرفق به مستنداته تحت مسؤوليته قبل الجلسة المحددة لنظر الدعوي بثلاثة أيام على الأقل.

وتجدر الإشارة إلي إنه يمكن أن يتم إبلاغ المدعي عليه بالدعوي من قلم الكتاب من خلال البريد الرقمي² أو رسالة علي تليفونه المحمول والمنزلي إذا كان قلم الكتاب قد علم بتلك البيانات من المدعي ، فيرسل قلم الكتاب إلي المدعي عليه رسالة من خلال البريد الرقمي للمحكمة موضعاً به الرقم الكودي الذي يستطيع من خلاله الاطلاع علي الدعوي والمستندات المرفقة ، والرد من خلاله بدفوعه وطلباته ، ويتم تبادل المذكرات ومتابعة قرارات المحكمة رقمياً.

1 راجع في ذلك : د/ رمزي سيف ، الوجيز في قانون المرافعات المدنية والتجارية المصري ، الطبعة الأولى ، مكتبة الكتب العربية ، 1957 ، ص 418 .

2 عرفت المادة الأولى من قانون رقم 175 لسنة 2018 البريد الإلكتروني بأنه:

البريد الإلكتروني : (وسيلة لتبادل رسائل إلكترونية علي عنوان محدد ، بين أكثر من شخص طبيعي أو اعتباري ، عبر شبكة معلوماتية ، أو غيرها من وسائل الربط الإلكترونية، من خلال أجهزة الحاسب الآلي وما في حكمها .)

أما في حالة عدم علم المدعي بمحل إقامة المدعي عليه أو بريده الرقمي أو تليفونه، يقوم قلم كتاب المحكمة من خلال الربط الرقمي بين موقع المحكمة وقاعدة بيانات مصلحة الأحوال المدنية بطلب الحصول على بيانات المدعي عليه حتي يتسنى مخاطبته وإبلاغه بالدعوي .

يقوم قلم كتاب المحكمة رقمياً بإخطار قلم المحضرين بنفس المحكمة حتي يتولى إعلان صحيفة الدعوي بتاريخ الجلسة المحددة لنظرها ، وذلك في خلال ثلاثة أيام علي الأكثر من تاريخ تسليمها إليه من خلال الموقع الرقمي ، وتحكم المحكمة المرفوعة إليها الدعوي علي من تسبب من العاملين بقلم الكتاب أو المحضرين بإهماله في تأخير الإعلان بغرامة لا تقل عن مائتي جنيه ولا تجاوز ألفين جنيه ولا يكون الحكم بها قابلاً لأي طعن (قانون المرافعات م 68) .

الفرع الثاني

جزاء النقص أو الخطأ في البيانات المقدمة بطلب عرض النزاع

نص المشرع على البطلان في حالة تخلف بيانات الإعلان أو البيان المتعلق بتوقيع المحامي. أما بيانات الدعوي - عدا البيان الخاص بتوقيع المحامي - وبيانات التكليف بالحضور فلم ينص المشرع على البطلان عند تخلفها، ولكن طبقاً للمبدأ العام في البطلان فإن البطلان يترتب عند تخلف أحد هذه البيانات إذا لم تتحقق بسبب تخلفه الغاية من الشكل أو البيان المطلوب.

وعلي ذلك فجزاء تخلف أي بيان من البيانات المتعلقة بصحيفة الدعوي أو بالإعلان أو بالتكليف بالحضور هو البطلان، ولكن إذا ثبت تحقق الغاية من البيان الناقص فلا يحكم بالبطلان.

وهناك بيان واحد فقط لا يترتب البطلان علي تخلفه وهو بيان الموطن المختار للمدعي حيث يجوز للمدعي عليه إعلانه في قلم كتاب المحكمة.¹

وهنا يجب إيضاح إنه لن يكون هناك أي نقص في البيانات المقدمة كما هو في إجراءات التقاضي العادية، حيث إنه ستكون هناك حقول هامة يجب ملؤها في النماذج المعدة لذلك علي موقع المحكمة فإن لم يتم ملؤها لا يتم الإجراء ولا التسجيل الرقمي² ولن يتم قبول الطلب أو

1راجع في ذلك : أ.د/ الأنصاري حسن النيداني ، مرجع سابق ، ص137 www.pdfactory.com

2 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 بالتسجيل الإلكتروني علي انه :

السجل المعد إلكترونيًا بالمحاكم الاقتصادية لتقيد بيانات الجهات والأشخاص المنصوص عليها في المادة (17) من هذا القانون ووسيلة التواصل معهم والتي تمكن راغب الإعلان من إخطار الخصوم بالدعوي أو بالطلبات العارضة أو بالأحكام التمهيدية الصادرة فيها وهو ما يمكن الاستئناس به لتعريف التسجيل الإلكتروني بأنه :

استكمالاً كما ينص القانون وبالتالي فإن تلك الفرضية وهي النقص في البيانات لن تتواجد في ظل العمل بنظام رقمية إجراءات التقاضي.

أما عن الخطأ في البيانات التي تم تقديمها بطلب رفع الدعوى فإن تلك الفرضية قد تتواجد في بعض الأحوال، وفي هذا الصدد نجد أن قانون المرافعات المعمول به حالياً لم ينص علي البطلان في حالة إغفال أي بيان من البيانات المنصوص عليها بالمادة (63) من قانون المرافعات وهي ذات البيانات الواجب توافرها في ظل العمل بنظام التقاضي عبر الوسائط الرقمية ، وبالتالي فإنه عند الخطأ في أي من هذه البيانات يجب الرجوع للقاعدة العامة للبطلان المنصوص عليها بالمادة (20) من قانون المرافعات والتي تقضي بأن يكون الإجراء باطلاً متى شابه عيب لم يتحقق بسببه الغاية من الإجراء، ويجب ثبوت عدم تحقق الغاية من الإجراء حتي ولو نص القانون صراحة علي البطلان كجزء لإغفال أو الخطأ في إجراء معين.

ووفقاً لنص المادة (65) من قانون المرافعات فإنه يجب قبول قيد الدعوى إذا كانت مصحوبة بما يدل علي سداد الرسوم المقررة قانوناً أو إعفاء المدعي منها، ويجب في هذا الصدد أن يتم إعطاء المدعي مهلة محددة بنص القانون يتم سداد الرسوم المحددة قانوناً خلالها والتي تم إرسال قيمتها للمدعي مسبقاً، وتبدأ هذه المهلة من التاريخ الذي يتم فيه إرسال رسالة سواء نصية علي التليفون المحمول الخاص بالمحامي أو المدعي أو البريد الرقمي للمحامي أو المدعي.

ويلاحظ في هذا الصدد إنه إذا تم رفع الدعوى دون أداء الرسم المطلوب فإنها لا تقيد ، و لا تسري آثار رفع الدعوى إلا من تاريخ استكمال الرسم القانوني وعندئذ لا تسري آثار رفع

{السجل المعد إلكترونياً بالمحاكم المدنية لقيد بيانات الجهات والأشخاص المنصوص عليها في إجراءات التقاضي الإلكتروني ووسيلة التواصل معهم والتي تمكن راغب الإعلان من إخطار الخصوم بالدعوى أو بالطلبات العارضة أو بالأحكام التمهيدية} .

الدعوي إلا من الوقت الذي يستكمل فيه الرسم، فجزء عدم سداد الرسم ألا يتم نظر الدعوي وألا يتم تحديد جلسة لها منذ البداية، حيث إنه لا يترتب علي سداد الرسم المقرر جزاء البطلان لأن المخالفة المالية بعمل ما لا ينبني عليها بطلان هذا العمل.

ووفقا لنظام الدعوي رقميا فإنه لا يترتب علي عدم إيداع المستندات المؤيدة للدعوي مخالفة أي جزاء سواء كان بطلان أو سقوط .

حيث إنه إذا لم يقدم المدعي المستندات الدالة علي صحة ادعائه أثناء رفع الدعوي فإنه يجوز له تقديمها بعد ذلك في أية حالة كانت عليها الدعوي حتي قبل إقفال باب المرافعة في الدعوي.

المطلب الثالث

آثار المطالبة القضائية 1

علي قلم الكتاب الرقمي إثبات تاريخ طلب القيد في جميع الأحوال ، وإذا رأي قلم الكتاب عدم قيد صحيفة الدعوي لعدم استيفاء المستندات والأوراق الموضحة عالية بشكل صحيح ، قام بعرض الأمر علي قاضي الأمور الوقتية ليفصل فيه فوراً ، إما بتكليف قلم الكتاب بقيد الدعوي أو بتكليف طالب قيدها باستيفائها بشكل صحيح ، وذلك بعد سماع أقواله من خلال الموقع الرقمي والتواصل معه من خلاله ، فإذا قيدت صحيفة الدعوي تنفيذاً لأمر القاضي، اعتبرت مقيدة من تاريخ تقديم طلب القيد.

يرسل قلم الكتاب إلي المدعي عليه صحيفة الدعوي والمذكرة الشارحة لدعوي المدعي عليه ، ويخطر به بقيد الدعوي واسم المدعي وطلباته والجلسة المحددة لنظرها وتجدر الإشارة إلي أن إبلاغ المدعي عليه بالدعوي من قلم الكتاب يتم من خلال البريد الرقمي أو رسالة علي تليفونه المحمول أو المنزلي هذا بالإضافة إلي إعلامه عن طريق اقرب قسم شرطة إليه وهو إجراء سوف يتم فقط في المرحلة الأولى من التحول نحو الإجراء الرقمي لتحقيق اليقين الرقمي إلي حين يطمئن المواطنون إلي الدليل الرقمي . أما إذا كان قلم الكتاب قد علم بتلك البيانات من المدعي ، فيرسل قلم الكتاب إلي المدعي عليه رسالة من خلال البريد الرقمي للمحكمة موضحاً به الرقم الكودي الذي يستطيع من خلاله الاطلاع علي الدعوي والمستندات المرفقة ، والرد من خلاله بدفوعه وطلباته ، ويتم تبادل المذكرات ومتابعة قرارات المحكمة رقمياً.، ويدعوه إلي الاطلاع علي ملف الدعوي وتقديم مستنداته ومذكرة بدفاعه وعلي المدعي عليه أن يودع رقمياً قلم الكتاب مذكرة

1 -راجع في ذلك: د/ محمد صابر احمد ، " دور الحاسب الآلي في تيسير إجراءات التقاضي " ، مرجع

سابق، ص 138 وما بعدها ، وقد آثرنا الإشارة دون الإفاضة لعدم اتساع المجال لذلك.

بدفاعه ويرفق به مستنداته تحت مسؤوليته قبل الجلسة المحددة لنظر الدعوي بثلاثة أيام علي الأقل.

أما في حالة عدم علم المدعي بمحل إقامة المدعي عليه أو بريده الرقمي أو تليفونه ، يقوم قلم كتاب المحكمة من خلال الربط الرقمي بين موقع المحكمة وقاعدة بيانات مصلحة الأحوال المدنية بطلب الحصول علي بيانات المدعي عليه حتي يتسنى مخاطبته وإبلاغه بالدعوي.

يقوم قلم كتاب المحكمة رقمياً بإخطار قلم المحضرين بنفس المحكمة حتي يتولى إعلان صحيفة الدعوي بتاريخ الجلسة المحددة لنظرها ، وذلك في خلال ثلاثة أيام علي الأكثر من تاريخ تسليمها إليه من خلال الموقع الرقمي ، وتحكم المحكمة المرفوعة إليها الدعوي علي من تسبب من العاملين بقلم الكتاب أو المحضرين بإهماله في تأخير الإعلان بغرامة لا تقل عن مائتي جنيه ولا تجاوز ألفين جنيه ولا يكون الحكم بها قابلاً لأي طعن.

ولا تعتبر الخصومة منعقدة في الدعوي إلا بإعلان صحيفتها إلي المدعي عليه ما لم يحضر يوم الجلسة .

متى قدمت المطالبة القضائية على الوجه المتقدم، فإن آثار قانونية عديدة تترتب على

ذلك، ويمكن تقسيم هذه الآثار على مستوى الفرعين التاليين :

الفرع الأول

الآثار الإجرائية للمطالبة الرقمية

يترتب على مجرد إيداع الصحيفة وقيدتها الآثار الإجرائية¹ التالية :

1- نشأة الخصومة أمام القضاء :

المقرر في قضاء محكمة النقض أنه وفقاً للمادة ٦٣ من قانون المرافعات يتعين لإجراء المطالبة القضائية إيداع صحيفة افتتاح الدعوى وهو ما يترتب عليه كأثر إجرائي بدء الخصومة وتعتبر الدعوى مرفوعة أمام القضاء ومنتجة لكل آثار المطالبة القضائية بمجرد إيداع صحيفة قلم الكتاب، أما إعلان الخصم بها فقد أصبح إجراءً منفصلاً ومستقلاً بذاته عن رفع الدعوى وتالياً وذلك كشرط لانعقاد الخصومة، والمقصود به إعلام الخصوم برفع الدعوى وبموضوع المنازعة تحقيقاً لمبدأ المواجهة بين الخصوم، بمعنى أن إجراء رفع الدعوى مستقل عن إجراء إعلانها، انعقاد الخصومة، وأن المشرع أوجب على المحكمة أن تراقب من تلقاء نفسها صحة إعلان الخصم الغائب - المادتان ٦٨ (٣) و ٨٥ من قانون المرافعات - وعلى ذلك فإن إعلان الخصم الغائب بصحيفة الدعوى في غير موطنه من شأنه أن يحول دون علمه بالدعوى وحضوره أمام القضاء، الأمر الذي يفوت الغاية من إعلان هذه الصحيفة فيترتب على ذلك بطلان أى إجراء أو حكم يصدر فيها.

المقرر في قضاء محكمة النقض أنه وفقاً للمادة ٦٣ من قانون المرافعات يتعين لإجراء المطالبة القضائية إيداع صحيفة افتتاح الدعوى وهو ما يترتب عليه كأثر إجرائي بدء الخصومة وتعتبر الدعوى مرفوعة أمام القضاء ومنتجة لكل آثار المطالبة القضائية بمجرد إيداع صحيفة قلم الكتاب، أما إعلان الخصم بها فقد أصبح إجراءً منفصلاً ومستقلاً بذاته عن رفع الدعوى وتالياً وذلك كشرط لانعقاد الخصومة، والمقصود به إعلام الخصوم برفع الدعوى وبموضوع المنازعة تحقيقاً لمبدأ المواجهة بين الخصوم، بمعنى أن إجراء رفع الدعوى مستقل عن إجراء إعلانها، انعقاد الخصومة، وأن المشرع أوجب على المحكمة أن تراقب من تلقاء نفسها صحة إعلان الخصم الغائب - المادتان ٦٨ (٣) و ٨٥ من قانون المرافعات - وعلى ذلك فإن إعلان الخصم الغائب بصحيفة الدعوى في غير موطنه من شأنه أن يحول دون علمه بالدعوى وحضوره أمام القضاء، الأمر الذي يفوت الغاية من إعلان هذه الصحيفة فيترتب على ذلك بطلان أى إجراء أو حكم يصدر فيها.

راجع فى ذلك : (الطعن رقم ٦٨٤٠ لسنة ٧٧ قضائية، الدوائر التجارية - جلسة 2019/06/11، منشور على

موقع محكمة النقض المصرية : https://www.cc.gov.eg/civil_judgments)

وهذا الأثر هو أهم أثر يترتب على تقديم لادعاء إلى القاضي، إذ انه يحرك نشاطه وتبدأ الخصومة بهذه المطالبة القضائية. ولذا يرتب القانون آثاراً بالنسبة للقاضي وأعوانه والخصوم تفرض عليهم السير في إجراءاتها .

2- تثبيت المحكمة المختصة :

يترتب على تقديم صحيفة الدعوى إلى قلم كتاب محكمة معينة، أن تصبح وحدها هي المختصة بالفصل فيها (والفرض أن هذه المحكمة مختصة وفقاً للقانون)، لأن ذلك من شأنه نزع الاختصاص عن باقي المحاكم الأخرى التي كانت مختصة بها (قبل رفع الدعوى) وفقاً للقانون .

3- تحديد سلطة المحكمة بما ورد في الطلب:

فالمطالبة القضائية هي التي تحدد نطاق الخصومة محلاً وسبباً وأشخاصاً، ولذا تتحدد سلطة القاضي فيما يتعين عليه الفصل فيه بما يقدم له من طلبات .

الفرع الثانى

الآثار الموضوعية للمطالبة الرقمية

وهى الآثار التي تتصل بحق المدعى المطلوب حمايته، وهى آثار يكمن أساسها في اعتبار

المطالبة القضائية بمثابة عمل تحفظي لحق المدعى وهذه الآثار هي :

1- قطع التقادم¹ :

تتقطع بتقديم الطلب مدة التقادم السارية لمصلحة المدعى عليه، ويبقى التقادم مقطوعا ما

بقيت الخصومة إلى أن يحكم فيها ، وتتقطع مدة التقادم، ولو رفع الطلب إلى الطلب إلى محكمة

غير مختصة .

2- اعذار المدعى عليه :

تعد المطالبة القضائية بمثابة أعذار للمدعى عليه، وتسرى من ثم كافة الآثار التي تترتب

على الأعذار منذ وقت المطالبة القضائية .

1 أن مفاد نص المادة ٣٨٣ من القانون المدنى يدل على أن إقامة الدعوى بإجراء صحيح أي بإيداع صحيفتها قلم كتاب المحكمة مستوفية كافة بياناتها يترتب عليه قطع التقادم ولو كانت إجراءات إعلان هذه الصحيفة باطلة إذ لا يؤثر بطلان إعلان الصحيفة على صحة ذلك الإجراء السابق ويمتد الانقطاع بهذا السبب طوال الوقت الذى يستغرقه سير الدعوى ولا يزول إلا بعد الحكم فيها ، فإذا حكم في موضوعها بالدين وحاز الحكم قوة الأمر المقضي بدأ تقادم جديد مدته خمس عشرة سنة طبقا للمادة ٣٨٥ / ٢ من القانون المشار إليه أما إذا حُكم برفض الدعوى أو بانتهاء الخصومة بغير حكم في موضوعها كالحكم بعدم قبول الدعوى أو بطلان صحيفتها أو بترك الخصومة فيها أو بسقوطها أو بانقضائها فإن أثر الانقطاع يزول ويعتبر التقادم كأنه لم ينقطع ، وفى غير هذه الحالات فإن المطالبة القضائية تظل منتجة لأثرها في قطع التقادم .

راجع فى ذلك : (الطعن رقم ١٤٧٩٨ لسنة ٨٥ قضائية ، الدوائر المدنية - جلسة 2020/06/16، منشور على

موقع محكمة النقض المصرية ، https://www.cc.gov.eg/civil_judgments)

3- توارث بعض الحقوق غير القابلة للانتقال :

يترتب على تقديم الطلب توارث بعض الحقوق التي رفع طلب قضائي بشأنها، رغم أنها لا تنتقل أصلاً بالخلافة ، بمعنى أن هذه الحقوق لا تنتقل إلى الخلف إذا توفى السلف قبل المطالبة بها أمام القضاء، ولكنه إذا توفى بعد المطالبة بها أمام القضاء فإن الخصومة لا تنقضي بل تستمر في مواجهة الورثة .

4 -يصبح الحق المدعى متنازعا فيه :

بالمطالبة القضائية يصبح الحق محل هذه المطالبة متنازعا فيه، وهذا يجعله يخضع لأحكام التعامل في الحقوق المتنازع عليها .

المطلب الرابع

موقف النظم القضائية المقارنة

وعلى الرغم من المخاوف أو العواقب التي قد تواجه فكرة التحول إلى الرقمية في رفع الدعوي والإعلان إلا أن العديد من الدول أخذت بهذا النظام وإن كان بصورة غير كاملة باعتباره اختياريًا، الأمر الذي يجعلها في مرحلة البداية أو الاختبار علي حد تعبير الفقه وهو ما سنعرض له في عدد¹ من الدول علي النحو التالي:²

أولاً: الإيداع الرقمي للمستندات أمام محكمة أستراليا الاتحادية³ :

في أستراليا، ووفقاً لبرنامج رقمية الإجراءات الذي تبنته المحكمة الاتحادية، تنقسم مراحل تطور تقنية الإيداع الرقمي للمستندات إلى أربع مراحل رئيسية :

بدأت المرحلة الأولى في أكتوبر سنة ٢٠٠٠ ، وفيها كان قلم كتاب المحكمة يتلقى صحيفة الدعوي والأوراق والمستندات المؤيدة لادعاءات المدعي وأدلة الإثبات، وتحصيل الرسوم والمصاريف القضائية عبر موقع المحكمة الاتحادية الرقمي علي شبكة الإنترنت⁴، ثم يتولى قلم

1 راجع في ذلك : د/ محمود مختار ، بحث منشور بعنوان "الإيداع الإلكتروني ، مرجع سابق ، الجزء الأول ، ص 470 وما بعدها ، وراجع أيضا : د/ محمود مختار ، استخدام تكنولوجيا المعلومات لتيسير إجراءات التقاضي المدني ، ص 161 وما بعدها .

2 راجع في ذلك : (تاريخ آخر دخول علي الموقع: 2020/3/22)

– <https://customers.microsoft.com/en-us/story/adgm-azure-office365-dynamics365-uae>

3 Refer to that: (تاريخ آخر دخول علي الموقع: 2020/3/22)

– <http://www.austlii.edu.au/au/journals/Mur>،

– <http://www.austlii.edu.au/forms/search1.html>، FOCUS ،Melbourne ،October 2001)

– <http://www.aija.org.au/AIJAVSCL/AIJAVSCLtopic6.pdf> >.

4 راجع في ذلك : (تاريخ آخر دخول علي الموقع : 2020/9/22)

الكتاب طباعة هذه الأوراق القضائية والمستندات ليحدد دائرة المحكمة المختصة تبعا لطبيعة موضوع النزاع¹.

وفي المرحلة الثانية، والتي بدأت في مارس ٢٠٠١ ، لم يطرأ علي نظام العمل سوي تعديلات طفيفة، والتي تجسدت في تبسيط إجراءات استخدام تقنية الإيداع الرقمي لصحيفة الدعوي قلم كتاب المحكمة.

-
- <http://www.aph.gov.au/library/pubs/bd/1999-2000/2000BD064.htm>،
 - <http://scaleplus.law.gov.au/html/pasteact/3/3328/top.htm>
- ، وراجع أيضا قانون المعاملات الإلكترونية لعام 1999 موجز :
- <http://www.law.gov.au/www/securitylawHome.nsf/AllDocs/599C6BC95712D9E6C?A256B9D0016CB4B> ،OpenDocument

1 المعلومات المتعلقة بمشروع الإيداع الإلكتروني " :

http://www.bundesgerichtshof.de/BGH_ERV_Info_2001-11-20.pdf

فقلم كتاب المحكمة يتلقى صحيفة الدعوي وما يدعمها من أوراق ومستندات بدلا من طباعة

Microsoft

ABU DHABI GLOBAL MARKET COURTS
محاكم لسوق، أبوظبي العالمية

ADGM Courts

From their inception, Abu Dhabi Global Market Courts had a clear vision to be innovative in how a court interacts with parties and their lawyers. By using Microsoft Cloud solutions, they are true fully digital courts.

“
We set out to deliver the world's very first fully digital civil and commercial courts. Using Microsoft Cloud solutions, today we have transformed the global legal and judicial landscape.
”

Linda Fitz-Alan, Registrar and Chief Executive, ADGM Courts
<https://adgmcourts.com>

+ SIMPLIFIED & MODERN USER EXPERIENCE

+ REAL TIME COLLABORATION & SPEED TO RESOLUTION

+ COST EFFICIENCY & EFFECTIVENESS

+ PLATFORM ACCESSIBILITY 24/7 FROM ANYWHERE IN THE WORLD

Microsoft Azure, Dynamics 365 and Office 365

LINK TO THE FULL CASE STUDY
[HTTPS://WWW.ABUDHABICOURTS.COM](https://www.abudhabicourts.com)

هذه الأوراق القضائية في هيئة دعائم ورقية¹ عبر برنامج PDF ، ثم تأتي مرحلة التوزيع الرقمي لهذه الأوراق والمستندات علي دوائر المحكمة حسب طبيعة موضوع النزاع.²

1 ويعتبر تاريخ الإيداع ووقته هو التاريخ والوقت المسجلان علي خادم ملفات المحكمة من أجل نقل المعلومات. إشعار الإيداع الإلكتروني ، والذي يتم تحديد التاريخ والوقت في نص هذا الإشعار. لا يوجد في هذه القواعد ما يقتضي تقديم أي معلومات في محكمة الأعمال بالوسائل الإلكترونية أو يحول دون تقديم نسخة مادية من أي ورقة مع كاتب المحكمة العليا المناسب بالإضافة إلي الإيداع الإلكتروني. يجوز تقديم الإيداع الإلكتروني إلي المحكمة في أي وقت من النهار أو الليل.

2 يجب أن تكون جميع الوثائق المودعة إلكترونيا قابلة للتحويل إلي وسائط التخزين الإلكترونية ، دون فقد المحتوى أو تغيير شكله في المظهر. يكون التنسيق الخاص بالمواد المودعة إلكترونيا هو تنسيق المستندات المحمولة (PDF) أو أي صيغة معتمدة أخرى .

وجاءت المرحلتين الثالثة والرابعة لتغيير نظم العمل السارية في المرحلتين الأولى والثانية،

وهو ما ظهر جليا في : صورة (1)¹

أ - الإدارة الرقمية الكاملة للأوراق منذ لحظة إرسالها من المستخدم حتي وصولها لهيئة

المحكمة التي ستتولى نظر النزاع.

ب - حق المستخدم في تغيير أو إصلاح الأخطاء التي قد تشوب البيانات المتعلقة بالأوراق التي

سبق تقديمها.²

1 راجع في ذلك : (تاريخ آخر دخول علي الموقع : 2020/3/22)

– <https://customers.microsoft.com/en-us/story/adgm-azure-office365-dynamics365-uae>

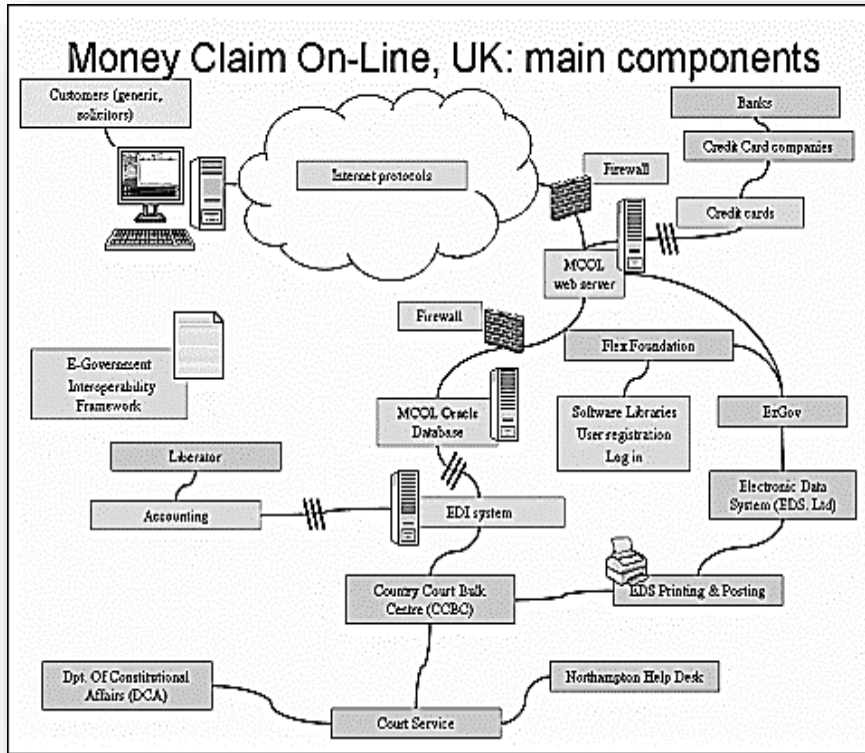
2 راجع في ذلك : (تاريخ آخر دخول علي الموقع : 2020/1/12)

– أسئلة وأجوبة حول القواعد التي تخول الخدمة الإلكترونية :

– http://www.uscourts.gov/Press_Releases/elecattach.pdf

ج- استخدام تقنية التوقيع الرقمي للمستندات والأوراق التي يود المستخدم إرسالها عبر تقنية

الإيداع الرقمي لقم كتاب المحكمة الموجود " Fees، Forms، Filings" ¹.



صورة (2)

للمستخدم الضغط علي رابط علي موقع المحكمة الاتحادية الاسترالية² ليختار النموذج الخاص بالورقة القضائية المراد تحريرها، وذلك من خلال ملئ البيانات الفارغة ، ثم إذا كانت البيانات

1 راجع في ذلك : كريستوفر كوهنر ، "متطلبات التوقيع الكتابي والمصادقة الإلكترونية: منظور مقارن" النظام المعقد للتوقيع المكتوب في القانون الألماني.

http://www.kuner.com/data/articles/signature_perspective.html (تاريخ آخر دخول علي

الموقع : 2019/12/12)

2 راجع في ذلك : (تاريخ آخر دخول علي الموقع : 2019/12/12)

<http://www.austlii.edu.au/au/journals/Mur>

الشخصية للمستخدم سبق تخزينها علي قاعدة بيانات الموقع الرقمي للمحكمة، فإنه لا يطلب منه - في حالة الدخول بعد ذلك - سوي إدخال أسم المستخدم وكلمة المرور . أما إذا كان مستخدم جديد، فإنه يجب عليه تحرير استمارة بيانات تتضمن كافة البيانات والمعلومات التي تحدد هوية المستخدم وتميزه عن غيره من المستخدمين¹.

ثم يظهر للمستخدم في نهاية خطوات إيداعه للمستندات رقم تعريفى ليستخدمه فيما بعد لمتابعة قضيته عبر الموقع الرقمي للمحكمة ويتعين علي المستخدم تقديم كافة الأوراق والمستندات في صيغة PDF والحفاظ علي الأصول الورقية لهذه المستندات التي يجب تقديمها . لهيئة المحكمة حال طلبها منه للاطلاع عليها وفحصها من قبل المحكمة .²

ثانياً: إنجلترا³

بخلاف القضايا قليلة القيمة والتي تقل قيمتها عن ١٠٠٠ يورو إذ يتم التعامل معها رقمياً، فإن المحاكم الأعلى درجة كمحاكم المقاطعات ، والمحكمة العليا بأقسامها بدأت في إتاحة التواصل الرقمي مع المحكمة عبر البريد الرقمي وذلك لرفع الدعاوي وإرسال الملفات ولقد تم إنشاء برنامج اتصال pilot project في ١١ محكمة من محاكم المقاطعات country court بهدف

1 راجع في ذلك : ساندر بورتر ، "نظرة عامة علي الإيداع الإلكتروني في أستراليا" عرض في مؤتمر :

_ AIJA ، VSCL LEGAL XML & ELECTRONIC FILING: THE AUSTRALIAN FOCUS ،Melbourne ،October 2001) p3 ، <http://www.aija.org.au/AJAVSCL/AJAVSCLtopic6.pdf>

2 جدير بالذكر أن الفارق بين تعديل الطلب الذي لا يرد إلا علي صحيفة مستوفاة لكافة بياناتها ثم تعدل الطلبات لسبب ما في حضور الخصم الآخر ، وبين تصحيح شكل الدعوي فهو يفترض أن صحتها معيبة فتؤجل لتصحيح شكلها كما لو رفعت دعوي علي أ الذي يتبين أنه توفي فتقطع الخصومة وتؤجل الدعوي لإعلان الورثة جميعا كل باسمه، راجع في ذلك : د/ محمود محمد هاشم، الخصومة أمام القضاء، بحث منشور في بعض المشكلات العملية في قانون المرافعات، إعداد مركز السنهوري للدراسات القانونية، ١٩٩٣ ، ص ١٦ .

3 راجع في ذلك : د/ فاطمة عادل سعيد ، التقاضي عبر وسائل التكنولوجيا والاتصال الحديث ، مرجع سابق ، الجزء الأول ، ص 385 .

استكمال وإيداع الأوراق رقمياً (ما يقارب ٢٠ صيغة مدنية) عبر الإنترنت، كما يتاح دفع مصروفات التقاضي عبر الإنترنت ببطاقات الائتمان وتبقي هذه الإجراءات المميكنة في حيز ضيق للتطبيق طالما لا يوجد إقبال متزايد عليها من المتعاملين مع مرفق العدالة، وفي بدايات عام ٢٠٠٦ زاد تطوير برنامج الاتصال الخاص بالمحاكم وقواعد البيانات ليؤمن مزيد من الحماية لسرية البيانات التي من شأنها أن تساهم في إنشاء ملف دعوي ويمكن من خلاله إيداع طلبات الخصوم an electronic case file رقمي ودفاعهم وقد تحكّم المحكمة بناء عليها إذا قدرت كفايتها وعدم وجود داع للمرافعات الشفوية، كما أقرت مصاريف مخفضة للتقاضي من خلال الإجراءات الرقمية في بعض المحاكم. أما فيما يتعلق بالمحكمة ذاتها فإنها لا تصدر إعلانات بصورة رسمية عبر الإنترنت ولكن من وقت لآخر بصورة غير رسمية كما لو أرسلت المحكمة بعض الإعلانات للخصوم أو مسودة للحكم الصادر عن القاضي، إلا أن مواعيد الجلسات وتاريخ انعقادها متاحة دائماً علي موقع المحكمة¹ مع الإشارة إلي أن أي تغيير في ميعاد الجلسات سيتم إخطار الأطراف به تليفونياً.

إلي جانب البرنامج السابق والذي يعتبر محل للتطور المتتابع² فيمكن إرسال صحف الدعاوي إلي المحكمة رقمياً عن طريقين أساسيين E- Filing الأول هو عن طريق البريد الرقمي

1 صورة (2) راجع في ذلك : (تاريخ آخر دخول علي الموقع : 2019/12/12)

– http://www.hmcourtsservice.gov.uk/onlineservices2/claim_process/make_claim.htm، visited 1 Desember 2019.

– <http://www.justice.gov.uk/courts/court-lists/list-companies-windingup>، last visited 9 October 2017.

2 بداية من العام ٢٠١٠ ظهر في العمل نظام أكثر تطوراً electronic working scheme يجب علي المتعاملين مع المحكمة عبر هذا النظام التأكد من ان كافة البيانات تم إرسالها في ملفات Pdf ، راجع في ذلك :

– https://www.justice.gov.uk/courts/procedure/rules/civil/rules/part05/pd_part05b، last visited on 10 October 2017.

فيرسل المدعي (المعلن) في هذه المرحلة بالبريد الرقمي الصحيفة إلي البريد الرقمي الخاص بالمحكمة غير إنه لن تتخذ أي إجراءات إلا بعد سداد الرسوم ، **الطريق الثاني** هي خدمة الصيغ عبر الإنترنت online forms service إذ يوجد علي موقع المحكمة عدد من الصيغ المعدة سلفا ويمكن استيفائها وإيداعها رقميا لدي المحكمة المختصة علي أن تكون الأخيرة تتوافر بها هذه الخدمة ويمكنها استقبال الدعاوي المرفوعة رقميا عبر موقع خدمة الصيغ عبر الإنترنت، ولقد وضعت قواعد عامة تحكم كلا من الطريقتين: فالمتقاضي الذي يستعمل تلك الخدمات لا يقع عليه التزام بأن يرسل بعد ذلك للمحكمة نسخة ورقية، ولا يعتبر الملف قد ارسل للمحكمة إلا بعد ان تستلمه خلال الوقت المحدد قبل الرابعة عصرا وإذا تم الإرسال بعد ذلك يعتبر الملف مرسل في اليوم التالي، وتقوم المحكمة بإرسال بريد رقمي تؤكد استلامها للملف، فإذا كانت الملفات الملحقة بالصحيفة التي يرسلها المدعي علي قدر من الأهمية أو يخشي علي سريتها فيرسلها علي مسؤوليته إذ لا يمكن ضمان الأمن ١٠٠ %، أو يتصل تليفونيا بالمحكمة ليلفت نظرها لذلك الملف.

ثالثا: الإيداع الرقمي للمستندات أمام القضاء الأمريكي¹ :

وفي ضوء المزايا المترتبة علي أعمال تقنية قلم كتاب المحكمة الرقمي في النظام القضائي، أخذ القضاء الفيدرالي الأمريكي بنظام معلوماتي لإيداع صحف الدعاوي " Electronic Case File Management والأوراق والمستندات التي تؤيد ادعاءات المدعي قلم كتاب المحكمة عبر الطريق الرقمي². فقد طبقت ٢١ محكمة فيدرالية في النظام القضائي الأمريكي³ نظام الإيداع

1 راجع في ذلك : (تاريخ آخر دخول : 2021/1/13)

— <http://www.austlii.edu.au/au/journals/MurUEJL/2002/42.html>

2 راجع في ذلك : (تاريخ آخر دخول : 2021/1/13)

— <http://www.mdd.uscourts.gov/content/civil-case-opening-procedures>

3 راجع في ذلك : (تاريخ آخر دخول : 2021/1/13)

— http://www.uscourts.gov/Press_Releases/elecattach.pdf

الرقمي للمستندات والأوراق¹، والتبادل الرقمي لها ، وهو ما أخذت به. أيضا ١١ من أصل ١٣ محكمة استئناف فيدرالية² كما يسمح هذا النظام المعلوماتي المعمول به أمام القضاء الفيدرالي الأمريكي بـكلاً من (وتري الباحثة انه في ظل التقاضي الرقمي يجب ان تتوفر هذه الخدمة عبر موقع المحكمة علي الصفحة الخاصة بكل قضية لكل من يطلبها من الخصوم) :

١. متابعة الخصوم لملف القضية، كمتابعة الطلبات القضائية ومذكرات الدفاع والدفع وتمكينهم من الاطلاع عليها ضمانا للرد عليها، والعلم بتاريخ الجلسات المخصصة لسماع الدعوي والتحقيق فيها بواسطة المحكمة.

٢. إخطار المدعي عليه رقميا بالأوراق المقدمة بواسطة المدعي، وذلك عبر البريد الرقمي الخاص به أو عبر تقنية الفاكس.

٣. حق الخصم في طلب تقارير عن القضية، وما وصلت إليه من تطورات³.

٤. يستطيع الخصم تصحيح البيانات والمعلومات التي أدلي بها أثناء تحريره للأوراق التي سبق تقديمها عبر الطريق الرقمي .

أ: يستلزم النظام الرقمي الذي تبنته المحاكم الفيدرالية الأمريكية أن يتوافر لدي المستخدم برامج معالجة النصوص "Microsoft Word". وخدمة الويب ، "Acrobat adobe" ومن الناحية العملية، يجهز المحامي الورقة الإجرائية علي الحاسب الآلي ثم يدخل علي الموقع الرقمي للمحكمة المختصة قانونا ، ثم يخزنها في صيغة PDF ، ثم بالضغط علي الرابط الخاص بتقديم

1راجع في ذلك: (تاريخ آخر دخول: 2021/1/13)

http://www.mdd.uscourts.gov/sites/mdd/files/CivilNOSDescriptions.pdf.

2refer to that:(تاريخ اخر دخول: 2021/1/13)

http://www.mdd.uscourts.gov/sites/mdd/files/SocialSecurityCasesProceduresManual.pdf

الأوراق رقمياً¹ تظهر شاشة إدخال اسم المستخدم والرقم السري ثم تظهر للمحامي خانة البيانات والمعلومات الواجب تحريرها بدقة مثل خطوات²: نوع المستند المراد تقديمه، ورقم القضية وغيرها وفي خلال يكون المحامي قد أتم إيداع ملف القضية المراد رقمياً تخطر المحكمة المدعي عليه بالأوراق المقدمة من المدعي عبر البريد الرقمي ويكون للمدعي عليه حق الاطلاع الرقمي علي هذه الأوراق ليتمكن من الرد عليها إعمال لمبدأ المواجهة بين الخصوم³ ومع ذلك إذا كان حق الاطلاع للمدعي عليه مجاناً في المرة الأولى، فإن الاطلاع التالي بمقابل مادي يعادل 07. دولار للورقة الواحدة. كما يجوز التقدم بطلب الإعفاء من الإيداع الرقمي⁴.

رابعا: الإيداع الرقمي للمستندات أمام القضاء الفرنسي⁵ :

يتسع نطاق التبادل الرقمي للأوراق والمستندات بين المحامي والمحكمة المدنية الفرنسية ليشمل محاكم الدرجة الأولى ومحاكم الدرجة الثانية⁶. فالاتصال الرقمي بين محامي الخصوم

1 راجع في ذلك : (تاريخ آخر دخول: 2021/1/13)

— <http://www.uscourts.gov/cmecf/cmecf.html>

2 راجع في ذلك : (تاريخ آخر دخول: 2021/1/13)

— Charles Lane ، Anthrax Scare Prompts Supreme Court E-filing Discussions
Washington Post 17.12.2001 ،
http://www.infowar.com/law/01/law_121701c_j.shtml.

3 راجع في ذلك : (تاريخ آخر دخول: 2021/1/13)

— <http://www.courts.state.co.us/iis/projects/efile/iisefile.htm>

4 يجوز للمحامي في قضية تخضع للإيداع الإلكتروني أن يطلب إعفاء القضية من شروط الإيداع الإلكتروني وإجراءاته عن طريق تقديم اقتراح يحدد أسباب الطلب. سيتم منح طلبات الإعفاء فقط لسبب وجيه. عند تقديم المستندات في حالة معفاة من الإيداع الإلكتروني ، قم بعمل تدوين بين قوسين في التسمية التوضيحية تحت رقم الحالة "الإعفاء من ECF". راجع في ذلك : (تاريخ آخر دخول: 2021/1/13)

— <http://www.mdd.uscourts.gov/sites/mdd/files/SocialSecurityCasesProceduresManual.pdf>

5 Refer to that : (تاريخ آخر دخول: 2021/1/13)

— https://e-justice.europa.eu/content_european_case_law_identifier_ecli-175-en.do

6 Refer to that : 2021/1/13: (تاريخ آخر دخول: 2021/1/13)

— <https://www.esens.eu/content/e-justice>

ومحاكم الاستئناف الفرنسية معمول به منذ عام 2003 ، في محاكم الاستئناف بحيث يستطيع المحامي تحرير صحيفة الاستئناف وإرسالها رقميا لقلم كتاب المحكمة المختصة الذي يتولى بعد ذلك إخطار المحامي بكتاب مسجل بعلم الوصول بقبول صحيفة الاستئناف أم لا، وذلك بعد فحص مضمون الرسالة الرقمية المتضمنة لصحيفة الاستئناف.

وهو ما يسري علي كافة أوراق المرافعات المعمول بها أمام محاكم الاستئناف الفرنسية¹، فلم ينحصر نطاق العمل الرقمي علي حق المستخدم(وكيل المستأنف) علي تحرير صحيفة الاستئناف وإيداعها قلم الكتاب رقميا، وإنما يحق له تقديم ما يؤيد صحيفة الاستئناف من مستندات وأوراق رقميا لتأييد صحة طعنه علي حكم محكمة أولي درجة².

كذلك، في نطاق محاكم الدرجة الأولى الفرنسية، أبرمت محكمة باريس الابتدائية ونقابة المحامين 2003/10/6 ، اتفاق بمقتضاه يجوز للمحامي الاطلاع الرقمي علي ملف الدعوي، والتبادل مع قلم كتاب المحكمة كافة الأوراق والمستندات رقميا، وتقديم طلب تحديد جلسة مستعجلة لنظر قضيته .

خامسا: الإيداع الرقمي للمستندات أمام القضاء الفنلندي³

1 <https://www.esens.eu/content/e-document>

2 Refer to that : (تاريخ آخر دخول: 2021/1/13)

3 <https://www.out-law.com/en/articles/2018/may/deal-with-data-risks-in-the-boardroom-or-pay-in-the-courtroom>

2Refer to that : Sophia BINET، L'utilisation des nouvelles technologies dans le procès civil op. cit.، p .24 2 Ibid.، p .24

3 Refer to that : La gestion du temps dans les systèmes judiciaires : une étude sur l'Europe، du nord، commission Européenne pour l'efficacité de la justice CEPEJ، sous la direction de : Mme Mirka Smolej، et M. Jon T. Johnsen، op. cit. p. 49op.

3Refer to that : (تاريخ آخر دخول: 2021/1/13)

4 https://e-justice.europa.eu/content_european_case_law_identifier_ecli-175-en.do

أقام القضاء الفنلندي نظامين من النظم الرقمية لتبسيط إجراءات التقاضي وتيسير مباشرتها من قبل ذوي الشأن. الأول TUOMAS ويطلق علي النظام الرقمي الخاص بإدارة الملف القضائي أمام المحكمة ، في حين أن النظام الثاني "SANTRA" نظام يتعلق بتلقي المحاكم للمطالبات القضائية عبر المواقع الرقمية الخاصة بها علي شبكة الإنترنت ويبدأ تحريك المتقاضي لدعواه عبر إرسال صحتها والمستندات المؤيدة والذي يتولى بعد ذلك توجيهها عبر البريد الرقمي لنظام SANTRA التي يتولى إدخال القضية المحكمة المختصة. ثم يأتي دور نظام "TUOMAS" في قاعدة البيانات الخاصة بالمحكمة لتتحدد الدائرة التي ستضطلع بالفصل في النزاع، وما يتبع ذلك من إجراءات حتي يتحقق اتصال هيئة المحكمة بالدعوي علي الوجه الصحيح قانونا.

و يتم إخطار الخصوم بتاريخ الجلسات المحددة لنظر الدعوي - مستخدما البريد الرقمي عبر نظام TUOMAS الخاص بهم ، وتكليفهم بالحضور أمام هيئة المحكمة لسماع أقوالهم ومناقشتهم فيما يقدمونه من طلبات وأوجه دفاع ودفع جوهريه.

ولا يتدخل العنصر البشري في عمل النظامين السابقين، فالإرسال الرقمي للأوراق القضائية والمستندات التي يتقدم بها الخصوم يتم بصورة رقمية فلا يتدخل أحد في SANTRA أو نظام THOMAS تلقائيه سواء في مرحلة إرسال ملف الدعوي للمحكمة المختصة أو إرسال التكليف بالحضور للمدعي عليه ، وإنما يتم ما سبق بصورة تلقائية، وبشكل رقمي .

يقوم النظام الرقمي (TUOMAS) بتخزين المستندات المرفقة بالدعوي في الذاكرة الرئيسية للحاسب ليتمكن القاضي من استرجاعها بسهولة حال الحاجة إليها .

كما يتولى هذا النظام الرقمي التخزين الصوتي لما دار من مناقشات بين الخصوم أثناء الجلسات، وما صدر عنهم من أقوال، وتسجيل شهادة الشهود أثناء تحقيق الدعوي، وذلك بدلا من

نظام محاضر الجلسات الورقية ليتمكن الخصوم بعد ذلك من إعادة سماع ما دار في الجلسات من خلال الضغط علي الرابط الخاص بسماع الجلسات.

سادسا: الإيداع الرقمي للمستندات أمام القضاء السنغافوري¹:

أخذ القضاء السنغافوري بنظام الإيداع الرقمي لصحيفة الدعوي Electronic Filing

"System (EFS) وما يدعمها من أوراق ومستندات في نطاق القضايا المدنية. وبمقتضى هذا

النظام الرقمي، يلتزم مورد الخدمات الرقمية في هذا المقام² :

1. تلقي الأوراق والمستندات الرقمية من محامي الخصوم، وإعادة إرسالها للمحكمة.
2. إخطار المدعي عليه أو محاميه حسب الأحوال بالأوراق التي قدمها المدعي عبر الطريق الرقمي ضمانا لصحة الإجراءات وعدم الإخلال بحقوق الدفاع.
3. تمكين الخصوم من الاطلاع الرقمي علي ملف الدعوي كاملا بما يتضمنه من أوراق حتي يتحقق العلم الكامل بملف القضية، وما يحويه من أوراق ومستندات .

كما شدد النظام القضائي السنغافوري - منذ عام ٢٠٠٠ - علي وجوب الإيداع الرقمي

للمستندات والأوراق عبر تقنية قلم الكتاب الرقمي في غالبية القضايا المدنية، فليس للمتناضي حق تقديم أوراق الدعوي والمستندات إلا في صورة رقمية .

سابعا: الإيداع الرقمي للمستندات أمام القضاء البرازيلي³:

1 راجع في ذلك : (تاريخ آخر دخول: 2021/1/13)

— <http://braddellbrothers.com/litigation.html>

2 راجع في ذلك : (تاريخ آخر دخول: 2021/1/13)

— <http://www.singaporelaw.sg/sglaw/laws-of-singapore/overview/chapter-2>

3 راجع في ذلك : د/ محمود مختار ، بحث منشور بعنوان "الإيداع الإلكتروني ، مرجع سابق ، الجزء الأول ، ص 476 .

بالنسبة للنظام القضائي في البرازيل، أخذ القليل من المحاكم البرازيلية بذلك حيث طبقت غالبية محاكم القضاء البرازيلي نظام الاطلاع الرقمي للقضايا من قبل الخصوم ووكلائهم من خلال كلمة المرور الخاصة بكل متقاضي يريد متابعة ما صدر في قضيته من قرارات عبر الموقع الرقمي للمحكمة المختصة .

ثامنا :الإيداع الرقمي للمستندات أمام القضاء الكندي ¹:

يتقارب النظام الرقمي المعمول به في القضاء الكندي مع النظام الأمريكي، فكلاهما يجيز إعمال تقنية الإيداع الرقمي للمستندات أمام محاكم الدرجة الأولى ومحاكم الدرجة الثانية. كما يجوز للمتقاضي الاطلاع علي ملف الدعوي وليس الإيداع الرقمي للأوراق فحسب ليتمكن من استدراك ما قد يشوب الأوراق من نقص أو خطأ في تحريرها

تاسعا: الوضع في القضاء المصري ²:

لم يأخذ النظام القضائي المصري بتقنية قلم الكتاب الرقمي علي النحو السابق إيضاحه، وإنما ينحصر ما قام به هذا النظام القضائي في إنه أوجب علي المتقاضي أو وكيله الذهاب لمقر المحكمة المختصة ليرفع دعواه من مكان واحد، ويطلق عليه نظام الشباك الواحد حيث يتم مراجعة صحيفة الدعوي وحفظ المستندات، وتقدير ودفع الرسوم، وتحديد الدائرة التي ستنتظر الدعوي، وتاريخ الجلسة في ربع ساعة فقط.³

1 راجع في ذلك : د/ محمود مختار ، بحث منشور بعنوان "الإيداع الإلكتروني ، مرجع سابق ، الجزء الأول ، ص 477 .

2 راجع في ذلك : د/ محمود مختار ، بحث منشور بعنوان "الإيداع الإلكتروني ، مرجع سابق ، ص 477 وما بعدها .

3 راجع في ذلك : د/ محمد صابر احمد ، " دور الحاسب الآلي في تيسير إجراءات التقاضي " ، مرجع سابق ، ص 110 .

وتتركز مساوئ النظام الورقي لقيود الدعاوي، والذي كانت تأخذ به المحاكم المصرية، في

الآتي :

- تأخر القضايا لحين قيدها في السجل المعد لذلك .
- تأخر في إسناد القضايا للدائرة المختصة .
- احتمال الخطأ عند إدخال البيانات وهو ما يمكن تجنبه حال إدخال تكنولوجيا المعلومات في نطاق العمل القضائي المصري، كما قد تؤدي إلي تحقيق المزايا

الآتية :

1. قلة عدد الموظفين اللازم لقيود القضايا في السجل المعد لذلك في المحكمة .
2. سرعة تلقي القضايا وإحالتها للدائرة المختصة .
3. الحد من الوقت المستهلك لعرض القضية علي الدائرة المختصة .
4. تمكين المختصين من الحصول علي تقارير وإحصاءات عن حالة القضايا في أي وقت .

▪ الخدمات الرقمية للمحاكم المصرية :

أطلقت وزارة العدل المصرية¹، بالتعاون مع وزارة الدولة لشئون التنمية الإدارية، مشروع ميكنة المحاكم (يشمل النيابة العامة وقضاء التحقيق) لوضع برامج حاسوبية لإدارة ملفات الدعاوي علي الحاسب الآلي، وذلك من خلال موقع الحكومة المصرية لتقديم خدمات القضاء العادي رقميا لجمهور المتقاضين، كخدمات محكمة النقض، وخدمات محاكم الاستئناف، وخدمات

1 راجع في ذلك :

المحاكم الابتدائية، وخدمات المحاكم الاقتصادية، والخدمات التي تقدمها مكاتب التسوية التابعة لمحاكم الأسرة.¹

وهو ما يعني أن خدمات محكمة النقض² ومحاكم الاستئناف والمحاكم الابتدائية متاحة الآن علي الإنترنت ، ويستطيع كل من المتقاضي والمحامي الحصول علي ما يريده من خدمات الاستعلام أو الحصول علي الشهادات الرسمية، أو الاطلاع عليها من المنزل أو المكتب كما يجوز للمتقاضي أو ممثله القانوني الحصول علي الخدمات القضائية السابقة من خلال منافذ تقديم الخدمات " المكاتب الأمامية" الموجودة بالمحاكم. كما أن محاكم الاستئناف تقدم بعض خدماتها عن طريق التليفون المحمول، وجاري دراسة إمكانية الحصول علي بعض الخدمات من خلال رسائل قصيرة يتم إرسالها علي التليفون المحمول ويلاحظ علي الخدمات المقدمة رقميا بواسطة محاكم القضاء العادي الاتي:

١ عدم فورية تلك الخدمات :

فليس بمقدور المستخدم الحصول علي الخدمة التي يرغب فيها لمجرد إدخاله للبيانات المطلوبة علي الوجه الصحيح، بل عليه الانتظار فترة زمنية تستغرق ما بين ثلاثة إلي خمس أيام عمل حتي يتسلم المستند المراد عن طريق البريد العادي بالنسبة لخدمات الحصول علي أوراق. أما بالنسبة لخدمات الاطلاع، فيجب علي المستخدم إدخال بريده الرقمي لاستقبال المستند المراد الاطلاع عليه.

1 راجع في ذلك :د/ محمد صابر احمد، " دور الحاسب الآلي في تيسير إجراءات التقاضي " ، مرجع سابق، ص110 .

2 راجع في ذلك : موقع محكمة النقض المصرية : www.cc.gov.eg

ولكن يستثني مما سبق خدمات الاستعلام التي يعقب إدخال المستخدم للبيانات ظهور

نتيجة البحث المرغوبة¹.

٢ النطاق المحدود :

يذكر أن الخدمات السابقة لا تقدمها كافة محاكم القضاء العادي²، فهناك محاكم لم يتم ميكنة خدماتها مثل المحاكم المتخصصة، كالمحاكم الاقتصادية باستثناء محكمة القاهرة الاقتصادية ومحاكم الأسرة ومكاتب التسوية التابعة لهم فليس بمقدور المتقاضي الحصول علي الخدمات السابقة من تلك المحاكم الأخيرة إلا بواسطة الآليات التقليدية القائمة علي ذهاب المتقاضي أو وكيله إلي مقر المحكمة، وما قد يترتب علي ذلك من مشقة وجهد ومال.

كما أن هذه الخدمات لا تقدمها كافة المحاكم الابتدائية³، فهناك ١٩ محكمة ابتدائية من أصل ٤٠ محكمة تم ميكنة خدماتها رقميا و ١٣ مأمورية تابعة للمحاكم الابتدائية وليس كافة المأموريات، أما محاكم الاستئناف، فهناك محكمة استئناف قنا لم يتم ميكنة خدماتها حتي الآن، فضلا عن ميكنة مأموريات استئناف فحسب.

٣ الحصول علي الخدمة وليس تقديمها⁴:

استنادا لطبيعة الخدمات السابقة، نجد أن المستخدم لمواقع المحاكم السابقة علي شبكة الإنترنت لا يستطيع تقديم المستندات أو الأوراق المتاحة رقميا إلي هيئة المحكمة، وإنما له الحق

1 راجع في ذلك : د/ محمد صابر احمد، " دور الحاسب الآلي في تيسير إجراءات التقاضي "، مرجع سابق، ص110.

2 راجع في ذلك : د/ محمود مختار، بحث منشور بعنوان "الإيداع الإلكتروني، مرجع سابق، الجزء الأول، ص 480.

3 راجع في ذلك : د/ محمد صابر احمد، " دور الحاسب الآلي في تيسير إجراءات التقاضي "، مرجع سابق، ص110.

4 راجع في ذلك : د/ محمود مختار، بحث منشور بعنوان "الإيداع الإلكتروني، مرجع سابق، الجزء الأول، ص 480.

في الحصول عليها فحسب، بمعنى أن تلك الخدمات تسير في اتجاه واحد، ألا وهو الحصول عليها وليس تقديمها لهيئة المحكمة.

كما يجوز استخدام الموبايل للاستعلام عن قرارات الجلسات بمحكمة النقض، أو للاستعلام عن وجود طعون مدنية أو جنائية من عدمه. وفي محاكم الاستئناف، يجوز الاستعلام هاتفيا عن وجود استئناف للحكم أو تظلم من قرار.

٤ لا ترد علي مرحلة نظر الدعوي¹ :

كذلك، لا يقدر المتقاضى أو محاميه على تقديم طلباته والمستندات المؤيدة لها، أو تقديم مذكرة بدفاعه عبر الموقع الرقمي للمحكمة، أو مناقشة الخصوم عبر شبكة الإنترنت، أو مناقشة الخبر فيما قدمه من تقارير لهيئة المحكمة، وإنما كل ما يملكه هو الحصول علي الخدمات السابقة بعد إتباع التعليمات الإرشادية وإدخال البيانات علي نحو صحيح.

٥ مجانية بعض الخدمات² :

تتباين الخدمات المقدمة بواسطة محاكم النظام القضائي المصري من حيث المقابل المادي، فخدمة الاستعلام مجانية ؛ لأنها تتيح معرفة تفاصيل وبيانات الدعوي من خلال رقم تعريفى يحصل عليه كل صاحب قضية ومحاميه. كذلك الحال بالنسبة لخدمات الاطلاع ، فهي مجانية أيضا.

1 راجع في ذلك : د/ محمود مختار ، بحث منشور بعنوان "الإيداع الإلكتروني ، مرجع سابق ، الجزء الأول ، ص 481 .

2 راجع في ذلك : د/ محمود مختار ، بحث منشور بعنوان "الإيداع الإلكتروني ، المرجع السابق ، ص 481 ، وراجع أيضا : د/ محمود مختار ، استخدام تكنولوجيا المعلومات لتيسير إجراءات التقاضي المدني ، ص 171 وما بعدها .

أما خدمات الحصول علي الشهادات من الدعاوي والصور الرسمية من الأحكام، فلها رسوم محددة، ويتم تسليم الشهادات والصور عن طريق المنافذ بالمحاكم أو بالبريد، ويتم دفع الرسوم عند الاستلام.

يمكن القول من العرض السابق إن إيداع صحف الدعاوي رقميا يوجد في العديد من الدول لكن المسئلة الرئيسية التي تواجه هذه الخطوة هي الشكالية فهل تستوفي رفع الدعوي عن طريق تسجيلها لدي موقع المحكمة¹ الشكل الذي تطلبه القانون حتي يعتد بالمطالبة القضائية؟

لم تغفل النظم الإجرائية² عن ذلك لذا نجد أن مسألة التوثيق في غاية الأهمية للاستيثاق من هوية الشخص رافع الدعوي ومنعا لإساءة استعمال الخدمة فتلجأ الأنظمة إلي واحد من ثلاثة حلول إما عن طريق قبول إيداع صحيفة الدعوي رقميا طالما تتم بواسطة المحامي أو أحد موظفي المحكمة المختصين أو تطلب التوقيع الرقمي وتذييل الأوراق به، أو كما هو الوضع في بعض الدول تكتفي بإجراء بسيط وهو كلمة مرور وكلمة السر الخاصة بكل متقاضي وهو ما سيتم طرحه لاحقا .

1 راجع في ذلك : (تاريخ آخر دخول: 2021/1/13)

— <https://news.microsoft.com/en-xm/2016/10/30/how-digital-justice-is-transforming-the-justice-system>

2 راجع في ذلك :

– The Great Disruption? Melbourne Legal Studies Research:

– Paper Series No. 897/

تاريخ آخر دخول علي الموقع : (<https://www.researchgate.net/publication/346579193>) (2021/1/8)

المبحث الثاني

أمن المعلومات¹

مصادقية الوسائل التكنولوجية الحديثة في مجال الاتصال عن بُعد تتجلي في الدقة التقنية للنظام المعلوماتي، وما يقدمه من أمن لمستخدميه، كما ذكر أحد الفقهاء .

وحيث إن إدخال نظم المعلومات والاتصالات إلي نطاق قضاء الدولة مرهون بإجراءات حماية مستندات الدعوي المقامة رقميا والتي تهدف إلي تقادي تعديل أو تغيير أو تدمير ملفاتها سواء تم ذلك عمدا أو بإهمال وضمان سرية وخصوصية المعلومات التي يدلي بها الخصوم في قضاياهم، فلا يجب أن تطغي غاية تسريع وتيرة التقاضي أمام قضاء الدولة من خلال هذه الآليات التقنية علي احترام المبادئ الأساسية للتقاضي، والتي لا يخرج عنها عدم إفشاء أسرار المتقاضين أو التعرض لها من قبل الغير . فقد تنتهك خصوصيات وأسرار المتقاضين حال تداول أوراق قضاياهم عبر شبكة الإنترنت، مما يقتضي وضع كل ما يضمن عدم تعرض الغير لهذه الخصوصيات، أو انتهاك أسرار الخصوم خاصة الأسرية أو أسرارهم التجارية والصناعية مما قد يضر مراكزهم الاقتصادية. ولذلك يجب علي النظم القضائية اتخاذ التدابير التكنولوجية التي تحول دون العبث بمصالح المتقاضين بالدخول علي الصفحات الرقمية التي تحوي ما قدموه من أوراق ومستندات .

فقد تتعرض المواقع الرقمية لمحاكم الدولة علي الإنترنت للتخريب، أو استبدال البيانات، أو يتم الاستيلاء علي المعلومات الخاصة بالمتقاضي طالب الخدمة كالاستيلاء علي أمواله عن طريق

1 راجع في ذلك :

Mikl s Kengyel; Zolt n Nemess nyi; International: Electronic technology and civil procedure : new paths to justice from around the world,p233.

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

معرفة أرقام بطاقات الائتمان، وهو ما يوجب وضع برامج حماية للشبكات دائم التحديث من قبل المسؤولين يصعب اختراقه حفاظًا علي خصوصية المتقاضين.

أما بالنسبة لأمن البيانات والذي بات غاية لا تدرك ولكن لابد إلا تترك ولا بد من ضمان تحقيقها علي مستوي رقمية الإجراءات في كافة مراحل الدعوي ودرجات التقاضي . وهو ما نهجه المشرع المصري بقانون جرائم المعلومات رقم 175 لسنة 2018 حيث عمل علي توفير الدعامة القانونية اللازمة لتحقيق الضوابط اللازمة لضمان سرية وأمن البيانات ، ففي مجال نقل البيانات تتبدي المخاطر المهددة للخصوصية والتي تتمثل في عدم قدرة شبكات الاتصال علي توفير الأمان المطلق أو الكامل لسرية ما ينقل عبرها من بيانات، حيث لم توفر برامج الحماية وسائل الأمان الكاملة والأكيدة من هذه المخاطر.

وفي مجال رقمية الإجراءات والتحول بالعدالة إلي الرقمية أهمية بالغة للوقوف علي مفهوم أمن المعلومات وسلامة البيانات لمعرفة التحديات المعاصرة التي تواجه أنظمة المعلومات وتجنب التعرض لها في مجال رقمية الإجراءات وهو ما سيكون محور ما سنعرض علي النحو التالي :

المطلب الأول: معايير أمن المعلومات وسلامة البيانات

المطلب الثاني : المخاطر التي تواجه الحق في الخصوصية في بيئة الإنترنت

المطلب الثالث: التحديات التي تواجه أنظمة أمن المعلومات واستراتيجياتها والحماية القانونية

المطلب الرابع: موقف النظم القضائية المقارنة

المطلب الأول

معايير أمن المعلومات وسلامة البيانات

أمن المعلومات¹ هو مصطلح سابق علي وجود المعلومات والبيانات في صورتها الحالية الرقمية او الرقمية ارتبط بالمعلومة بغض النظر عن الوسيلة التي تحملها او تنقل من خلالها او تخزن فيها .

هذا وتتعدد تعريفات أمن المعلومات وتتنوع حسب زاوية النظر إليها، فيمكن تعريفه² من الناحية الأكاديمية بأنه هو العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من مخاطر الاعتداء عليها ، اما من الناحية التقنية فهي الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات، وأخيرا من الزاوية القانونية فهي تلك التشريعات التي تهدف إلي مكافحة الاعتداء علي المعلومات ومعاينة مرتكبي الاعتداء بهدف توفير الردع .

وبناء علي ما سبق يمكن القول إن أمن المعلومات هو تلك الرؤي والسياسات والإجراءات التي تصمم وتنفذ علي مستويات مختلفة، فردية ومؤسسية ومجتمعية، وتستهدف تحقيق عناصر الحماية والصيانة المختلفة التي تضمن أن تتحقق للمعلومات السرية أو الموثوقية، أي التأكد من أن المعلومات لا تُكشف ولا يُطلع عليها من قبل أشخاص غير مخولين بذلك ، وفي هذا المجال سوف نعرض لاحقا لما يلي :

الفرع الأول: المعايير الواجبة لتوافر أمن المعلومات في النظام

الفرع الثاني: أمن المعلومات وسلامة البيانات

1 راجع في ذلك : الباحث / حسين خلف موسي، استراتيجية أمن المعلومات في ظل حروب الجيل السادس ، خاص لمركز شُرُفات لدراسات العولمة والإرهاب ، عمان ،الأردن 9 مارس، 2017 ، ص 2 .

2 راجع في ذلك : المحامي/ يونس عرب، أمن المعلومات ماهيتها وعناصرها واستراتيجياتها ، بحث منشور علي موقع : http://www.arablaw.org/Download/Information_Security.doc ، بتاريخ :

2015/7/15 ، العنوان الإلكتروني للموقع : <http://www.arablaw.org> ، ص 1- 2 .

الفرع الأول

المعايير الواجبة لتوافر أمن المعلومات في النظام¹

1- السرية: Confidentiality

النظام الآمن هو النظام الذي يضمن سرية وخصوصية² البيانات المخزنة فيه، وبالتالي إتاحة هذه البيانات فقط لأصحابها المصرح لهم بالتعامل معها ، إضافة إلي تأمين الطرق المناسبة لحمايتها من القراءة أثناء نقلها عبر شبكة الاتصال وتبادلها ويمكن تحقيق سرية نقل المعلومات من خلال تشفير الرسائل المتبادلة بمفاتيح معينة ، ويحقق ذلك من خلال مجموعة من الطرق تقدم مستويات مختلفة من درجات الأمان وسرعة نقل المعلومات³.

2- التكاملية: Integrity

يضمن النظام الآمن تكاملية البيانات المخزنة فيه ، ويقصد بالتكاملية حماية البيانات من عمليات الحذف والتحريف⁴ ، ويتم تأمين ذلك من خلال مجموعة من الأساليب توفرها نظم قواعد المعطيات

1 راجع في ذلك : القاضي/ حاتم جعفر ، دور التقاضي الإلكتروني في دعم وتطوير العدالة قراءة في الواقع الحالي والنتائج المتوقعة ، دور التقاضي الإلكتروني في دعم وتطوير العدالة قراءة في الواقع الحالي والنتائج المتوقعة ، مؤتمر المناخ القضائي الداعم للإستثمار، الأسكندرية فبراير 2015 ، ص6 وما بعدها ، و راجع أيضا : د/ يونس عرب، أمن المعلومات ماهيتها وعناصرها ، مقال منشور على شبكة الانترنت. <http://www.abhatoo.net.ma/%D8%A7%D9%84%D> ، ص2-3 .

2 راجع في ذلك :

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

3 راجع في ذلك : تأمين خدمات الويب من التشفير إلي البنية التحتية لأمان خدمة الويب علي موقع : <https://docplayer.net/18946782-Securing-web-services-from-encryption-to-a-web-service-security-infrastructure.html> (تاريخ آخر دخول علي الموقع 2020/9/22)

4 راجع في ذلك :

كقوائم النفاذ والصلاحيات بالإضافة إلي علاقات الترابط Referential Integrity ما بين البيانات المخزنة فيها. كما يؤمن النظام الآمن تكامل البيانات المرسله لمعرفة فيما إن تم تعديل أو حذف أي جزء منها أو إنها غير مكررة ، وتحقيق ذلك يمكن أن يتم من خلال توليد مفتاح أو جواز مرور (توقيعاً) للرسالة المرسله " توقيع رقمي " ¹ ، باستخدام بعض الخوارزميات، مثل خوارزمية MD5 أو خوارزمية SHA ، وتضمنين إذن المرور هذا مع كل رسالة ترسل عبر الشبكة، وبالتالي التأكد من أن الرسالة صحيحة ولم يتم العبث بها.

3- التوفر والإتاحة: Availability

يؤمن النظام الآمن استمرارية وصول المستخدمين إلي المعطيات الخاصة بهم دون أي

-
- دليل المستخدم النموذجي لتطبيق التحقق من التأمين عبر الإنترنت :
 - <https://docplayer.net/8406020-Model-user-guide-for-implementing-online-insurance-verification.html> (تاريخ آخر دخول علي الموقع 2020/9/22)
 - تفاعل خدمات الويب الآمن الموثوق به GRA الإصدار 1.2 :
 - <https://docplayer.net/13164367-Gra-reliable-secure-web-services-service-interaction-profile-version-1-2-table-of-contents.html> (تاريخ آخر دخول علي الموقع 2020/9/22)
 - تسجيل الدخول الأحادي الجديدة لـ IBM Lotus Notes & Domino IBM Corporation
 - <https://docplayer.net/10464389-New-single-sign-on-options-for-ibm-lotus-notes-domino-2012-ibm-corporation.html> (تاريخ آخر دخول علي الموقع 2020/9/22)
 - CPNI VIEWPOINT تكوين وإدارة الوصول الآمن عن بعد لأنظمة التحكم الصناعية :
 - <https://docplayer.net/15929126-Cpni-viewpoint-configuring-and-managing-remote-access-for-industrial-control-systems.html> (تاريخ آخر دخول علي الموقع 2020/9/22)
- 1 راجع في ذلك :
- واجهة خدمة ويب التوقيع الرقمي :
 - <https://docplayer.net/15095840-Digital-signature-web-service-interface.html> (تاريخ آخر دخول علي الموقع 2020/9/22)
 - أمن الرسائل الفورية :
 - <https://docplayer.net/680438-Instant-messaging-security.html> (تاريخ آخر دخول علي الموقع 2020/9/22)

تأخير. ولهذه الخاصية عدد من السمات المتمثلة في: المقاومة Resistance وهي قدرة النظام علي الحفاظ علي نفسه من العمليات التي تجعله غير متاح للمستخدمين المخولين باستخدامه و المقدره علي التوسع لسد الحاجات المستقبلية Scalability ؛ والمرونة Flexibility المتمثلة في توفر الإمكانيات والأدوات التي تمكن من إدارة النظام دون أن يستدعي ذلك إلي توقعه، وسهولة الاستخدام ، ويعتمد بناء نظام معلوماتي آمن للتقاضي¹ الرقمي علي توافر المتطلبات السابقة إضافة للالتزام بالمعايير العالمية فيما يخص الأرشفة والاسترجاع وحفظ ومعالجة المعلومات² وبما يحقق دوماً الممارسات الآمنة للمعلومات بما يحقق ويوفر الثقة

1 راجع في ذلك : المحامي د/ يونس عرب ، جرائم الكمبيوتر والإنترنت إيجاز في المفهوم والنطاق والخصائص والصور والقواعد الإجرائية للملاحقة والإثبات ، ورقة عمل مقدمة الي مؤتمر الأمن العربي 2002 ، تنظيم المركز العربي للدراسات والبحوث الجنائية ، أبو ظبي 10-12/ 2002/2/ ، ص16 وما بعدها.

2 راجع في ذلك :

- دليل صانع القرار لتأمين البنية التحتية لتكنولوجيا المعلومات :
- <https://docplayer.net/14248162-A-decision-maker-s-guide-to-securing-an-it-infrastructure.html> (تاريخ آخر دخول علي الموقع 2020/9/22)
- <https://docplayer.net/13010656-This-working-paper-provides-an-introduction-to-the-web-services-security-standards.html> (تاريخ آخر دخول علي الموقع 2020/9/22)
- نظرة عامة علي أمان الشبكة :
- <https://docplayer.net/16983218-Overview-of-network-security-the-need-for-network-security-desirable-security-properties-common-vulnerabilities-security-policy-designs.html> (تاريخ آخر دخول علي الموقع 2020/9/22)
- خدمات الوكيل: إرشادات الممارسة الجيدة :
- <https://docplayer.net/17978767-Proxy-services-good-practice-guidelines.html> (تاريخ آخر دخول علي الموقع 2020/9/22)
- مبادئ وأسس خدمات الويب: نظرة شاملة (التقنيات ومحركات الأعمال والنماذج والبنية والمعايير)
- <https://docplayer.net/13788312-Principles-and-foundations-of-web-services-an-holistic-view-technologies-business-drivers-models-architectures-and-standards.html> (تاريخ آخر دخول علي الموقع 2020/9/22)
- المصادقة الآمنة والجلسة. إدارة الدولة لخدمات الويب :
- <https://docplayer.net/13164273-Secure-authentication-and-session-state-management-for-web-services.html> (تاريخ آخر دخول علي الموقع 2020/9/22)

المطلوبة للتعامل مع النظام والاعتماد عليه بداية من استخدام تقنيات التشفير مروراً بتأمين خصوصية المعلومات وذلك من خلال منع استخدامها في غير الغرض المرخص به من قبل صاحب المعلومة وختاماً تأمين سرية المعلومات عن طريق تحقيق الحماية لمحتوي البيانات ضد محاولات التغيير¹ والتعديل والمحو الإلتلاف مع ضمان التحقق من شخصية مستخدم النظام والمعلومات والتأكد من كونه مخول له التعامل فعلاً معه أو مرخصاً له بذلك ، ويسبق ذلك كله وجود الوعي البشري اللازم لدي مستخدمي النظام بأهمية امن المعلومات وعدم الاستهانة به.

1 راجع في ذلك :

- نظرة عامة حول الأمان لمشاركة الملفات المتنقلة الآمنة من فئة المؤسسات :
- <https://docplayer.net/11363722-Security-overview-enterprise-class-secure-mobile-file-sharing.html> (تاريخ آخر دخول علي الموقع 2020/9/22)
- Notes on Network Security – Introduction: <https://docplayer.net/13999066-Notes-on-network-security-introduction.html> (تاريخ آخر دخول علي الموقع 2020/9/22)
- Summary of Technical Information Security for Information Systems and Services Managed by NUIT (Newcastle University IT Service) : <https://docplayer.net/10015902-Summary-of-technical-information-security-for-information-systems-and-services-managed-by-nuit-newcastle-university-it-service.html> (تاريخ آخر دخول علي الموقع 2020/9/22)
- عمليات تبادل رسائل خدمات الويب الموثوقة الآمنة وإثبات العبث :
- <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)

الفرع الثاني

أمن المعلومات وسلامة البيانات¹

لحفاظ علي أمن وسلامة المعلومات والبيانات يجب معرفة العناصر الأساسية لنظام الأمن المعلوماتي ، و البرمجيات المستخدمة في تشغيل النظام هذه النقاط الهامة سنعرض لها علي النحو التالي :

أولاً : الحفاظ علي أمن وسلامة المعلومات والبيانات²

قد تنتهك خصوصيات وأسرار المتقاضين حال تداول أوراق قضاياهم عبر شبكة الإنترنت، مما يقتضي وضع كل ما يضمن عدم تعرض الغير لهذه الخصوصيات، أو انتهاك أسرار الخصوم خاصة الأسرية أو أسرارهم التجارية والصناعية مما قد يضر بمراكزهم الاقتصادية³.

1 راجع في ذلك : جمال محمد غيطاس ، الأمن المعلوماتي والجرائم الإلكترونية أدوات جديدة للصراع ، مقال منشور علي موقع مركز الجزيرة للدراسات : <https://tasharuk.net/ar/resources/index.php?id=657> ، 1 مارس 2012 ، ص 1 وما بعدها .

2 راجع في ذلك : د/ محمود مختار ، استخدام تكنولوجيا المعلومات لتيسير إجراءات التقاضي المدني ، مرجع سابق ، ص 85 وما بعدها .

3 راجع في ذلك :

– Osama ahmed Attalla ، is the legal protection of digital privacy enough in Egypt’’? ، previous reference ، p 9 .

فمصادقية الوسائل التكنولوجية الحديثة في مجال الاتصال عن بُعد تتجلي في الدقة التقنية للنظام المعلوماتي، وما يقدمه من أمن لمستخدميه¹.

ولهذا، شدد كلا من التشريع الأمريكي والكندي علي أن إدخال نظم المعلومات والاتصالات إلي نطاق قضاء الدولة مرهون بضمان سرية وخصوصية المعلومات التي يدلي بها الخصوم في قضاياهم، فلا يجب أن تطغي غاية تسريع وتيرة التقاضي أمام قضاء الدولة من خلال هذه الآليات التقنية علي احترام المبادئ² الأساسية للتقاضي .

وهو ما أيدته توصيات اللجنة الوزارية للدول الأعضاء في الاتحاد الأوروبي (رقم 2003/15) ، حيث أوجبت علي الدول الأعضاء تيسير استخدام وسائل التكنولوجيا الحديثة لحفظ وتخزين الوثائق الرقمية المستخدمة في مجال التقاضي، وضمان عدم اختراق الغير لها، أو التلاعب بالتوقيعات الرقمية الخاصة بالخصوم أو وكلائهم³.

وذكرت الفقرة السادسة من المادة 748 من القانون الفرنسي رقم 1678 لسنة 2005، والصادر في 2005/12/28، والذي ينظم الاتصال عبر الآليات الرقمية لمباشرة الإجراءات

1راجع في ذلك : راجع في ذلك : المحامي/ يونس عرب، أمن المعلومات ماهيتها وعناصرها واستراتيجياتها ، بحث منشور علي موقع : http://www.arablaw.org/Download/Information_Security.doc ، بتاريخ : 2015/7/15 ، العنوان الإلكتروني للموقع : <http://www.arablaw.org> ، ص 1 ، وما بعدها ، وراجع أيضا : المهندس/ سعيد عطا الله ، ما الفرق بين الأمان والخصوصية، مقال منشور بتاريخ : 2020/5/14 ، ص1 وما بعدها ، علي موقع :

– <https://www.arageek.com/ما-الفرق-بين-الأمان-والخصوصية/>
2 راجع في ذلك : د/ محمد حسام محمود لطفي، استخدام وسائل الاتصال الحديثة في التفاوض علي العقود وإبرامها، 1993، بدون دار نشر، ص 40.

3 راجع في ذلك :

– Ali Rıza ÇAM، Première section une justice transparente et efficace، op. cit.، p.19

المدنية، وبعض إجراءات التنفيذ الجبري¹، إنه "يجب أن تضمن الإجراءات الفنية المتخذة — في ضوء الشروط والأوضاع المبينة بقرار وزير العدل — إمكانية تحديد هوية الخصوم في نطاق الاتصال الرقمي، وسلامة المستندات المرسلة، وأمن وسرية المبادلات، وحفظ عمليات النقل التي تمت، وتسمح بتحديد تاريخ الإرسال والاستلام من قبل المستلم بطريقة لا تقبل الشك"².

ولذلك، تتخذ النظم القضائية المقارنة³ التدابير التكنولوجية التي تحول دون العبث بمصالح المتقاضين بالدخول علي الصفحات الرقمية التي تحوي ما قدموه من أوراق ومستندات.

أما بالنسبة لأمن البيانات الذي بات غاية لآبد من تحقيقها في نطاق قضاء الدولة. فعلي "هيئة تنمية صناعة تكنولوجيا المعلومات ومركز حماية البيانات الشخصية" اتخاذ ما يلزم من

1 راجع في ذلك :

_ Fabrice CALVET La dématérialisation et la signification des actes d'Huissiers de justice ou la plus value en matière de transmission de l'information judiciaire، mémoire، UNIVERSITE LUMIERE LYON 2، Année universitaire 2007 / 2008، www.memoireonline.com/.../m_La-dématérialisation-et-la-signification، p.30

2 راجع في ذلك :

« Art. 748-6. - Les procédés techniques utilisés doivent garantir، dans des conditions fixées par arrêté du garde des sceaux، ministre de la justice، la fiabilité de l'identification des parties à la communication électronique، l'intégrité des documents adressés، la sécurité et la confidentialité des échanges، la conservation des transmissions opérées et permettre d'établir de manière certaine la date d'envoi et celle de la réception par le destinataire. »

3 راجع في ذلك : د / عمر عبد العزيز الدبور ، آليات تفعيل الحماية والوقاية من الجرائم الإلكترونية (إنشاء ضببية خاصة بالجرائم الإلكترونية) ، بحث مقدم الى المؤتمر العملى الدولي الحادي عشر - لكلية الحقوق - جامعة أسيوط الاتجاهات الحديث في القانون الإجرائي ، فى الفترة من 29 الى 30 مارس 2017) ، ص18 وما بعدها .

إجراءات واحتياطات، ووضع الضوابط اللازمة لتحقيق سرية وأمن البيانات، لحماية حقوق¹

الأشخاص المعنية بالبيانات ومن هذه الإجراءات :

1- عمل نسخ احتياطية من البيانات لحظيا وحفظها في مكان آخر².

1 حدد المشرع بالمادة 2،3 من قانون رقم ١٥١ لسنة ٢٠٢٠ بإصدار قانون حماية البيانات الشخصية ، حقوق

الشخص المعني بالبيانات وشروط جمع ومعالجة البيانات علي النحو التالي :

المادة (٢) :

(لا يجوز جمع البيانات الشخصية أو معالجتها أو الإفصاح عنها أو إفشائها بأي وسيلة من الوسائل إلا

بموافقة صريحة من الشخص المعني بالبيانات ، أو في الأحوال المصرح بها قانوناً .

ويكون للشخص المعني بالبيانات الحقوق الآتية :

١ - العلم بالبيانات الشخصية الخاصة به الموجودة لدي أي حائز أو متحكم أو معالج والاطلاع عليها والوصول إليها أو الحصول عليها .

٢ - العدول عن الموافقة المسبقة علي الاحتفاظ ببياناته الشخصية أو معالجتها .

٣ - التصحيح أو التعديل أو المحو أو الإضافة أو التحديث للبيانات الشخصية .

٤ - تخصيص المعالجة في نطاق محدد .

٥ - العلم والمعرفة بأي خرق أو انتهاك لبياناته الشخصية .

٦ - الاعتراض علي معالجة البيانات الشخصية أو نتائجها متي تعارضت مع الحقوق والحريات الأساسية

للشخص المعني بالبيانات . وباستثناء البند (٥) من الفقرة السابقة ، يؤدي الشخص المعني بالبيانات مقابل تكلفة

الخدمة المقدمة إليه من المتحكم أو المعالج فيما يخص ممارسته لحقوقه ، ويتولى المركز إصدار قرارات تحديد

هذا المقابل بما لا يتجاوز عشرين ألف جنيه) .

مادة (٣) :

(يجب لجمع البيانات الشخصية ومعالجتها والاحتفاظ بها ، توافر الشروط الآتية :

١ - أن تجمع البيانات الشخصية لأغراض مشروعة ومحددة ومعلنة للشخص المعني .

٢ - أن تكون صحيحة وسليمة ومؤمنة .

٣ - أن تعالج بطريقة مشروعة وملاتمة للأغراض التي تم تجميعها من أجلها .

٤ - ألا يتم الاحتفاظ بها لمدة أطول من المدة اللازمة للوفاء بالغرض المحدد لها .

وتحدد اللائحة التنفيذية لهذا القانون السياسات والإجراءات والضوابط والمعايير القياسية للجمع والمعالجة والحفظ

والتأمين لهذه البيانات) .

2 راجع في ذلك :

2- غرف ووحدات رقمية بديلة يمكن استئناف العمل من خلالها لو تعطل العمل بغرفة الكمبيوتر الرئيسية .

3- تحديث نظم التشغيل وقواعد البيانات والبرامج الضرورية لحفظ ومعالجة البيانات

4- لكل مستخدم رقم تعريفى وكلمة مرور خاصة به ، ويجب أن تكون كلمة المرور قوية وأمنة (مركبة من أحرف ورموز وأرقام) ، وأن لا يعطيها للغير .

5- وضع الضوابط الفنية اللازمة لنسخ أو تعديل أو حذف أي بيانات تتعلق بالقضية.

ثانيا : العناصر الأساسية لنظام الأمن المعلوماتي¹

إن النظام الأمني الفعال يجب أن يشمل جميع العناصر ذات الصلة بنظام المعلومات الرقمية و يمكن تحديد هذه العناصر بما يلي² :

أ. منظومة الأجهزة الرقمية و ملحقاتها :

- تأمين ودمج عمليات نقل الملفات عبر الإنترنت :
 - <https://docplayer.net/15798654-White-paper-securing-and-integrating-file-transfers-over-the-internet.html> (تاريخ آخر دخول علي الموقع 2020/9/22)
 - خدمة تسجيل الصوت الرقمي والنسخ للمحاكم :
 - <https://docplayer.net/7568151-In-the-subordinate-courts-of-the-republic-of-singapore-epractice-direction-no-2-of-2007-request-for-digital-audio-recording-transcription-service.html> (تاريخ آخر دخول علي الموقع 2020/9/22)
 - Oracle Database Backup Service .تأمين النسخ الاحتياطي في Oracle Cloud :
 - <https://docplayer.net/3130959-Oracle-database-backup-service-secure-backup-in-the-oracle-cloud.html> (تاريخ آخر دخول علي الموقع 2020/9/22)
- 1 راجع في ذلك : الباحث / حسين خلف موسي، استراتيجية أمن المعلومات فى ظل حروب الجيل السادس ، خاص لمركز شُرَفَات لدراسات العولمة والارهاب ، عمان ،الأردن 9 مارس، 2017 ، ص 4 وما بعدها .
- 2 راجع في ذلك : المحامي/ يونس عرب، أمن المعلومات ماهيتها وعناصرها واستراتيجياتها ، مرجع سابق، ص 1 وما بعدها .

إن أجهزة الحواسيب تتطور بشكل هائل وبالمقابل هناك تطور في مجال السبل المستخدمة لاختراقها مما يتطلب تطوير نظم الحماية وآلياتها و مهارات العاملين في أقسام المعلومات لكي يستطيعوا مواجهة حالات التلاعب و العبث المقصود في الأجهزة وغير المقصود.

ب. الأفراد العاملين في أقسام المعلومات (مسئولي حماية البيانات ،

وحائزها)¹

1 عرف المشرع بالمادة (1) من قانون رقم ١٥١ لسنة ٢٠٢٠ بإصدار قانون حماية البيانات الشخصية كلا من :
(الشخص المعني بالبيانات : أي شخص طبيعي تنسب إليه بيانات شخصية معالجة إلكترونيًا تدل عليه قانونًا أو فعلاً ، وتمكن من تمييزه عن غيره .

الحائز : أي شخص طبيعي أو اعتباري ، يحوز ويحتفظ قانونيًا أو فعليًا ببيانات شخصية في أي صورة من الصور ، أو علي أي وسيلة تخزين سواءً أكان هو المنشئ للبيانات ، أم انتقلت إليه حيازتها بأي صورة .

المتحكم : أي شخص طبيعي أو اعتباري يكون له بحكم أو طبيعة عمله ، الحق في الحصول علي البيانات الشخصية وتحديد طريقة وأسلوب ومعايير الاحتفاظ بها ، أو معالجتها والتحكم فيها طبقًا للغرض المحدد أو نشاطه .

المعالج : أي شخص طبيعي أو اعتباري مختص بطبيعة عمله ، بمعالجة البيانات الشخصية لصالحه أو لصالح المتحكم بالاتفاق معه ووفقًا لتعليماته (. كما حدد المشرع التزامات مسؤولي وحائزي البيانات علي النحو التالي :

أولاً : التزامات المتحكم مادة (٤) :

(مع مراعاة أحكام المادة (١٢) من هذا القانون ، يلتزم المتحكم بما يأتي :

١ - الحصول علي البيانات الشخصية أو تلقيها من الحائز أو من الجهات المختصة بتزويده بها بحسب الأحوال بعد موافقة الشخص المعني بالبيانات ، أو في الأحوال المصرح بها قانونًا .

٢ - التأكد من صحة البيانات الشخصية واتفاقها وكفايتها مع الغرض المحدد لجمعها

٣ - وضع طريقة وأسلوب ومعايير المعالجة طبقًا للغرض المحدد ، ما لم يقرر تفويض المعالج في ذلك بموجب تعاقد مكتوب .

٤ - التأكد من انطباق الغرض المحدد من جمع البيانات الشخصية لأغراض معالجتها .

٥ - القيام بعمل أو الامتناع عن عمل يكون من شأنه إتاحة البيانات الشخصية إلا في الأحوال المصرح بها قانونًا .

- ٦ - اتخاذ جميع الإجراءات التقنية والتنظيمية وتطبيق المعايير القياسية اللازمة لحماية البيانات الشخصية وتأمينها حفاظًا علي سريتها ، وعدم اختراقها أو إتلافها أو تغييرها أو العبث بها قبل أي إجراء غير مشروع
- ٧ - محو البيانات الشخصية لديه فور انقضاء الغرض المحدد منها ، أما في حال الاحتفاظ بها لأي سبب من الأسباب المشروعة بعد انتهاء الغرض ، فيجب ألا تبقي في صورة تسمح بتحديد الشخص المعني بالبيانات
- ٨ - تصحيح أي خطأ بالبيانات الشخصية فور إبلاغه أو علمه به .
- ٩ - إمساك سجل خاص للبيانات ، علي أن يتضمن وصف فئات البيانات الشخصية لديه ، وتحديد من سيفصح لهم عن هذه البيانات أو يتيحها لهم وسنده والمدد الزمنية وقيودها ونطاقها وآليات محو البيانات الشخصية لديه أو تعديلها وأي بيانات أخرى متعلقة بنقل تلك البيانات الشخصية عبر الحدود ووصف الإجراءات التقنية والتنظيمية الخاصة بأمن البيانات .
- ١٠ - الحصول علي ترخيص أو تصريح من المركز للتعامل مع البيانات الشخصية
- ١١ - يلتزم المتحكم خارج جمهورية مصر العربية بتعيين ممثل له في جمهورية مصر العربية وذلك علي النحو الذي تبينه اللائحة التنفيذية .
- ١٢ - توفير الإمكانيات اللازمة لإثبات التزامه بتطبيق أحكام هذا القانون وتمكين المركز من التفتيش والرقابة للتأكد من ذلك .
- وفي حال وجود أكثر من متحكم يلتزم كل منهم بجميع الالتزامات المنصوص عليها في هذا القانون ، وللشخص المعني ممارسة حقوقه تجاه كل متحكم علي حدة .
- وتحدد اللائحة التنفيذية لهذا القانون السياسات والإجراءات والضوابط والمعايير الفنية لتلك الالتزامات (.
- ثانيا : التزامات المعالج مادة (٥) :**
- (مع مراعاة أحكام المادة (١٢) من هذا القانون ، يلتزم معالج البيانات الشخصية بما يأتي :
- ١ - إجراء المعالجة وتنفيذها طبقاً للقواعد المنظمة لذلك بهذا القانون ولائحته التنفيذية ووفقاً للحالات المشروعة والقانونية وبناءً علي التعليمات المكتوبة الواردة إليه من المركز أو المتحكم أو من أي ذي صفة بحسب الأحوال ، وبصفة خاصة فيما يتعلق بنطاق عملية المعالجة وموضوعها وطبيعتها ونوع البيانات الشخصية واتفاقها وكفايتها مع الغرض المحدد له .
- ٢ - أن تكون أغراض المعالجة وممارستها مشروعة ، ولا تخالف النظام العام أو الآداب العامة .
- ٣ - عدم تجاوز الغرض المحدد للمعالجة ومدتها ، ويجب إخطار المتحكم أو الشخص المعني بالبيانات أو كل ذي صفة ، بحسب الأحوال ، بالمدة اللازمة للمعالجة .
- ٤ - محو البيانات الشخصية بانقضاء مدة المعالجة أو تسليمها للمتحكم .
- ٥ - القيام بعمل أو الامتناع عن عمل يكون من شأنه إتاحة البيانات الشخصية أو نتائج المعالجة إلا في الأحوال المصرح بها قانونًا .

- ٦ - عدم إجراء أي معالجة للبيانات الشخصية تتعارض مع غرض المتحكم فيها أو نشاطه إلا إذا كان ذلك بغرض إحصائي أو تعليمي ولا يهدف للربح ودون الإخلال بحرمة الحياة الخاصة .
- ٧ - حماية وتأمين عملية المعالجة والوسائط والأجهزة الإلكترونية المستخدمة في ذلك وما عليها من بيانات شخصية .
- ٨ - عدم إلحاق أي ضرر بالشخص المعني بالبيانات بشكل مباشر أو غير مباشر .
- ٩ - إعداد سجل خاص بعمليات المعالجة لديه ، علي أن يتضمن فئات المعالجة التي يجريها نيابة عن أي متحكم وبيانات الاتصال به ومسئول حماية البيانات لديه ، والمدد الزمنية للمعالجة وقيودها ونطاقها وآليات محو البيانات الشخصية لديه أو تعديلها ، ووصفًا للإجراءات التقنية والتنظيمية الخاصة بأمن البيانات وعمليات المعالجة .
- ١٠ - توفير الإمكانات لإثبات التزامه بتطبيق أحكام هذا القانون عند طلب المتحكم وتمكين المركز من التفتيش والرقابة للتأكد من التزامه بذلك .
- ١١ - الحصول علي ترخيص أو تصريح من المركز للتعامل علي البيانات الشخصية.
- ١٢ - يلتزم المعالج خارج جمهورية مصر العربية بتعيين ممثل له في جمهورية مصر العربية وذلك علي النحو الذي تبينه اللائحة التنفيذية .
- وفي حال وجود أكثر من معالج ، يلتزم كل منهم بجميع الالتزامات المنصوص عليها في هذا القانون وذلك في حال عدم وجود عقد يحدد التزامات ومسئوليات كل منهم بوضوح .
- وتحدد اللائحة التنفيذية لهذا القانون السياسات والإجراءات والضوابط والشروط والتعليمات والمعايير القياسية لتلك الالتزامات) .

ثالثا : شروط المعالجة مادة (٦) :

- (تعد المعالجة الإلكترونية مشروعة وقانونية في حال توفر أي من الحالات الآتية :
- ١ - موافقة الشخص المعني بالبيانات علي إجراء المعالجة من أجل تحقيق غرض محدد أو أكثر .
- ٢ - أن تكون المعالجة لازمة وضرورية تنفيذًا للالتزام تعاقدية أو تصرف قانوني أو لإبرام عقد لصالح الشخص المعني بالبيانات ، أو لمباشرة أي من إجراءات المطالبة بالحقوق القانونية له أو الدفاع عنها
- ٣ - تنفيذ التزام ينظمه القانون أو أمر من جهات التحقيق المختصة أو بناءً علي حكم قضائي . ٤ - تمكين المتحكم من القيام بالتزاماته أو أي ذي صفة من ممارسة حقوقه المشروعة ، ما لم يتعارض ذلك مع الحقوق والحريات الأساسية للشخص المعني بالبيانات) .

رابعا : الالتزام بالإخطار والإبلاغ مادة (٧) :

- (يلتزم كل من المتحكم والمعالج بحسب الأحوال حال علمه بوجود خرق أو انتهاك للبيانات الشخصية لديه بإبلاغ المركز خلال اثنتين وسبعين ساعة ، وفي حال كان هذا الخرق أو الانتهاك متعلقًا باعتبارات حماية الأمن القومي فيكون الإبلاغ فورياً ، وعلي المركز وفي جميع الأحوال إخطار جهات الأمن القومي بالواقعة فوراً ، كما يلتزم بموافاة المركز خلال اثنتين وسبعين ساعة من تاريخ علمه بما يأتي :

يلعب الفرد دوراً أساسياً و مهماً في مجال أمن المعلومات و الحواسيب و حيث ان له تأثير فعال في أداء عمل الحواسيب بجانبه الإيجابي و السلبي ، فهو عامل مؤثر في حماية الحواسيب و المعلومات و لكن في الوقت نفسه فإنه عامل سلبي في مجال تخريب الأجهزة و

- ١ - وصف طبيعة الخرق أو الانتهاك ، وصورته وأسبابه والعدد التقريبي للبيانات الشخصية وسجلاتها
 - ٢ - بيانات مسئول حماية البيانات الشخصية لديه .
 - ٣ - الآثار المحتملة لحادث الخرق أو الانتهاك .
 - ٤ - وصف الإجراءات المتخذة والمقترح تنفيذها لمواجهة هذا الخرق أو الانتهاك والتقليل من آثاره السلبية
 - ٥ - توثيق أي خرق أو انتهاك للبيانات الشخصية ، والإجراءات التصحيحية المتخذة لمواجهة
 - ٦ - أي وثائق أو معلومات أو بيانات يطلبها المركز .
- وفي جميع الأحوال يجب علي المتحكم والمعالج ، بحسب الأحوال ، إخطار الشخص المعني بالبيانات خلال ثلاثة أيام عمل من تاريخ الإبلاغ وما تم اتخاذه من إجراءات
- وتحدد اللائحة التنفيذية لهذا القانون الإجراءات الخاصة بالإبلاغ والإخطار) .

خامسا :التزامات مسئول حماية البيانات الشخصية مادة (٩) :

(يكون مسئول حماية البيانات الشخصية مسئولاً عن تنفيذ أحكام القانون ولائحته التنفيذية وقرارات المركز ، ومراقبة الإجراءات المعمول بها داخل كيانه الإشراف عليها ، وتلقي الطلبات المتعلقة بالبيانات الشخصية وفقا لأحكام هذا القانون . ويلتزم علي الأخص بالآتي :

- ١ - إجراء التقييم والفحص الدوري لنظم حماية البيانات الشخصية ومنع اختراقها ، وتوثيق نتائج التقييم وإصدار التوصيات اللازمة لحمايتها .
 - ٢ - العمل كنقطة اتصال مباشرة مع المركز وتنفيذ قراراته ، فيما يخص تطبيق أحكام هذا القانون .
 - ٣ - تمكين الشخص المعني بالبيانات من ممارسة حقوقه المنصوص عليها في هذا القانون .
 - ٤ - إخطار المركز في حال وجود أي خرق أو انتهاك للبيانات الشخصية لديه .
 - ٥ - الرد علي الطلبات المقدمة من الشخص المعني بالبيانات أو كل ذي صفة ، والرد علي المركز في التظلمات المقدمة إليه من أي منهما وفقا لأحكام هذا القانون .
 - ٦ - متابعة القيد والتحديث لسجل البيانات الشخصية لدي المتحكم أو سجل عمليات المعالجة لدي المعالج ، بما يكفل ضمان دقة البيانات والمعلومات المقيدة به .
 - ٧ - إزالة أي مخالفت متعلقة بالبيانات الشخصية داخل كيانه ، واتخاذ الإجراءات التصحيحية حيالها .
 - ٨ - تنظيم البرامج التدريبية اللازمة لموظفي كيانه ، لتأهيلهم بما يتناسب مع متطلبات هذا القانون .
- وتحدد اللائحة التنفيذية لهذا القانون الالتزامات والإجراءات والمهام الأخرى التي يجب علي مسئول حماية البيانات الشخصية القيام بها) .

سرقة المعلومات سواء لمصالح ذاتية أو لمصالح الغير، إن من متطلبات أمن الحواسيب تحديد مواصفات محددة للعاملين و وضع تعليمات واضحة لاختيارهم و ذلك للتقليل من المخاطر التي يمكن أن يكون مصدرها الأفراد إضافة إلي وضع الخطط لزيادة الحس الأمني و الحصانة من التخريب ، كما يتطلب الأمر المراجعة الدورية للتدقيق في شخصية وسلوك الأفراد العاملين من وقت لآخر و ربما يتم تغيير مواقع عملهم و محاولة عدم احتكار المهام علي موظفين محددين هذا بالإضافة إلي الرقابة عليهم من جانب رؤوسهم .

ثالثا : البرمجيات المستخدمة في تشغيل النظام

تعتبر البرمجيات من المكونات غير المادية لجهاز الحاسب الآلي Soft Wear و عنصر أساسي في نجاح استخدام النظام ، لذلك من الأفضل اختيار حواسيب ذات أنظمة تشغيل لها خصائص أمنية عالية الكفاءة والتي منها :

1- شبكة تناقل المعلومات :

تعتبر شبكة تناقل المعلومات المحلية أو الدولية ثمرة من ثمرات التطورات في مجالات الاتصالات كما إنها سهلت عملية التراسل بين الحواسيب و تبادل و استخدام الملفات ، و لكن من جهة أخرى إتاحة عملية سرقة المعلومات أو تدميرها سواء من الداخل كاستخدام الفيروسات أو من الخارج من خلال الدخول عبر منظومات الاتصال المختلفة ، لذلك لا بد من وضع إجراءات حماية و ضمان أمن الشبكات من خلال إجراء الفحوصات المستمرة لهذه المنظومات و مراقبتها و توفير الأجهزة الخاصة بالفحص و حسب طبيعة المنظومات و التطبيقات المستخدمة

يتم اتخاذ الإجراءات الاحترازية لحماية الموقع و تحصينه من أي تخريب أو اختراق¹ أو اعتراض².

كما يجب أن تعطي أهمية للمواقع والأبنية التي يتم تخزين أجهزة الحواسيب و ملحقاتها بها وتأمينها وصيانتها بما يتوافق وأهميتها .

1 (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) . راجع في ذلك : م1 قانون 175 لسنة 2018 .

2 (الاعتراض : مشاهدة البيانات أو المعلومات أو الحصول عليها بغرض التنصت أو التعطيل، أو التخزين أو النسخ، أو التسجيل ، أو تغيير المحتوى ، أو إساءة الاستخدام أو تعديل المسار أو إعادة التوجيه وذلك لأسباب غير مشروعة ودون وجه حق) . راجع في ذلك : م1 قانون 175 لسنة 2018 .

المطلب الثاني

المخاطر التي تواجه الحق في الخصوصية في بيئة الإنترنت²

تتزايد مخاطر التقنيات الحديثة علي حماية الخصوصية³ ، كتقنيات رقابة (كاميرات) الفيديو، وبطاقات الهوية والتعريف الرقمية، وقواعد البيانات الشخصية، ووسائل اعتراض ورقابة البريد والاتصالات، ورقابة بيئة العمل ، وبفعل الكفاءة العالية للوسائل التقنية والإمكانات غير المحدودة في مجال تحليل واسترجاع المعلومات، اتجهت جميع دول العالم بمختلف هيئاتها ومؤسساتها إلي إنشاء قواعد البيانات لتنظيم عملها، واتسع علي نحو كبير استخدام الحواسيب لجمع وتخزين ومعالجة البيانات الشخصية لأغراض متعددة فيما يعرف ببنوك ومراكز المعلومات الوطنية ، ومع تلمس المجتمعات لإيجابيات استخدام الحواسيب في هذا المضمار ظهر بشكل متسارع أيضا، الشعور بمخاطر تقنية المعلومات وتهديدها للخصوصية⁴ . هذا الشعور نما وتطور بفعل الحالات الواقعية للاستخدام غير المشروع للبيانات الشخصية واتساع دائرة الاعتداء علي حق الأفراد في حماية الحياة الخاصة مما حرك الجهود الدولية والإقليمية والوطنية لإيجاد مبادئ وقواعد من شأن مراجعاتها حماية الحق في الحياة الخاصة ، وبالضرورة إيجاد التوازن بين

1 راجع في ذلك : راجع في ذلك : أ.م.د.م.ني تركي و م.م. جان سيريل ، الخصوصية المعلوماتية وأهميتها ومخاطر التقنيات ،مجلة كلية بغداد للعلوم الاقتصادية الجامعة العدد الخاص بمؤتمر الكلية ، ص9 وما بعدها
2 راجع في ذلك : د/ جبالى أبو هشيمة كامل ، حماية البيانات الشخصية في البيئة الرقمية دراسة مقارنة بين القانون الفرنسي ومشروع القانون المصري ، بحث منشور بمؤتمر كلية الحقوق ،جامعة أسيوط ، 2016 ، ص9 وما بعدها .

3 راجع في ذلك : أ.م.د.م.ني تركي و م.م. جان سيريل ، الخصوصية المعلوماتية وأهميتها ومخاطر التقنيات ،مرجع سابق ، ص4 وما بعدها

4 راجع في ذلك : راجع في ذلك : أ.م.د.م.ني تركي و م.م. جان سيريل ، الخصوصية المعلوماتية وأهميتها ومخاطر التقنيات ، مرجع سابق ، ص9 وما بعدها

حاجات المجتمع لجمع وتخزين ومعالجة البيانات الشخصية ، وكفالة حماية هذه البيانات من مخاطر الاستخدام غير المشروع لتقنيات معالجتها¹.

وإذا كانت الجهود الدولية تتجه نحو الحماية التشريعية للحياة الخاصة²، وحمايتها من مخاطر استخدام الحواسيب ، فان هذا المسلك قد رافقه اتجاه متشائم لاستخدام التقنية في معالجة البيانات الشخصية. فالتوسع الهائل وبنوك المعلومات علي نحو خاص تمثل المسلك الصائب في مواجهة الأثر السلبي للتقنية علي الحياة الخاصة لاستخدام الحواسيب حيث أثار المخاوف من إمكانية انتهاك الحياة الخاصة، وممكن إثارة هذه المخاوف، أن المعلومات المتعلقة بجميع جوانب حياة الفرد الشخصية، كالوضع الصحي والأنشطة الاجتماعية والمالية والسلوك والآراء السياسية وغيرها، يمكن جمعها وتخزينها لفترة غير محددة، كما يمكن الرجوع إليها جميعا بمنتهى السرعة والسهولة، ومع الزيادة في تدفق المعلومات التي تحدثها الحواسيب، تضعف قدرة الفرد علي التحكم في المعلومات³.

وهذه النظرة كانت نظرة تبدو مبالغاً فيها، إلا إنها تعكس حجم التخوف من الاستخدام غير المشروع للتقنية، وتحديد الحواسيب، في كل ما من شأنه تهديد الحق في الحياة الخاصة .

1 راجع في ذلك : د/ راشد بن حمد البلوشي ، ورقة عمل يقدمها مقدمه الي المؤتمر الدولي الأول حول "حماية امن المعلومات و الخصوصية في قانون الإنترنت" ، مرجع سابق ، ص9 وما بعدها .

2 راجع في ذلك : د/ جمال عبده عبد العزيز سيد الجهود الدولية لمكافحة الجرائم المعلوماتية في اطار أدلة إثباتها في التشريعات العربية ، بحث مقدم الي المؤتمر العملي الدولي الحادي عشر- لكلية الحقوق - جامعة أسيوط الاتجاهات الحديث في القانون الإجرائي ، في الفترة من 29 الي 30 مارس 2017، ص9 وما بعدها

3 راجع في ذلك : د/ يونس عرب ، ورقة عمل " الاتجاهات التشريعية للجرائم الإلكترونية " ، ورشة عمل " تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية " ، هيئة تنظيم الاتصالات / مسقط - سلطنة عمان ، 2- 4 إبريل 2006 ، ص4 وما بعدها

مسألة الخصوصية بدأت تظهر مع انتشار استخدام أجهزة الحاسب الآلي في السبعينيات، حين تبين أن " إنَّ المعالجة الآلية للبيانات والمعلومات يمكن أن تتجم عنها مخاطر جدية تطال الحياة الخاصة للأفراد، خصوصاً إذا تمت هذه المعالجة من دون علم أصحابها أو موافقتهم الصريحة " ، والدول التي أدركت باكراً حجم هذه المسألة، بادرت منذ السبعينيات إلي إصدار تشريعات خاصة بحماية الحياة الخاصة . حيث عمدت هذه الدول، لا سيما الأوروبية منها، إلي تحديث تشريعاتها تبعاً، وذلك مع الالتزام بالغاية المحددة مسبقاً موضعاً أنّ من بين ما فرضته هذه التشريعات ، منح مجموعة من الأفراد حق الوصول إلي المعلومات لتصحيحها ، مع عدم التصرف بها من دون موافقة أصحاب المعلومات¹.

إنّ خرق² الخصوصية³ علي شبكة الإنترنت يمكن أن يتم من قبل جهات ثلاث أساسية هي مزود خدمة الاتصال (Internet Service Provider) ، والمواقع التي يزورها المتصفح ، بالإضافة إلي مخترقي الشبكة (Hackers) ، أفراداً أو أجهزة أمنية واستخباراتية . إن باستطاعة مزود الخدمة أن يرصد كل ما تقوم به علي الإنترنت (مكان وزمان الدخول إلي الشبكة، المواقع التي تم تصفّحها، الكلمات التي جري البحث عنها، الحوارات، الرسائل الرقمية المتبادلة... إلخ) ، وذلك من خلال رقم الإنترنت الخاص بالمستخدم وهي برمجيات قادرة علي تحليل كل حركة تجري علي الشبكة الرقمية وأدوات آخري تعرف بال «Proxy» و «Packet» (Internet

1 راجع في ذلك : د/ جبالي أبو هشيمة كامل ، : حماية البيانات الشخصية في البيئة الرقمية دراسة مقارنة بين القانون الفرنسي ومشروع القانون المصري ، بحث منشور بمؤتمر كلية الحقوق ، جامعة اسبوط ، 2016 ص 12 وما بعدها .

2 راجع في ذلك : أ.م. د/ مني تركي و م.م. جان سيريل ، الخصوصية المعلوماتية وأهميتها ومخاطر التقنيات ، مجلة كلية بغداد للعلوم الاقتصادية الجامعة العدد الخاص بمؤتمر الكلية 2013 ، ص 9 ما بعدها

3 راجع في ذلك : أ.م. د/ مني تركي و م.م. جان سيريل ، الخصوصية المعلوماتية وأهميتها ومخاطر التقنيات ، مرجع سابق ، ص 4 ما بعدها.

(Protocol)¹. وهو ما يمكن أن يتم أيضا بسبب تحميل وتنصيب تطبيقات الهاتف المحمول والتي تتم وللأسف بإذن صاحب البيانات كشرط للحصول علي التطبيق او الدخول إلي الموقع . فالعديد إن لم يكن كافة المواقع التفاعلية وتحديداً مواقع النشاط التجاري والتجارة الرقمية علي الإنترنت²، تتطلب من المستخدم تقديم وتعبئة نموذج يتضمن معلومات مختلفة ، سواء أكان في معرض الاشتراك بخدمات معينة او التسجيل او الانضمام لمجموعات النقاش او حتي لإجراء تعليق او إرسال رسالة او تحميل أي تطبيق من تطبيقات الموبايل . وتتضمن مادة هذه المعلومات اسم المستخدم وعنوانه للعمل والمنزل وأرقام الهاتف والفاكس وعنوان البريد الرقمي ومعلومات حول السن والجنس والحالة الاجتماعية ومكان الإقامة والدخل الشهري او السنوي واحياناً اهتمامات الشخص، وأما مواقع البيع والشراء علي الإنترنت والمواقع التي يتم فيها إجراء عمليات دفع فإنها تتطلب رقم بطاقة الاعتماد ونوعها وتاريخ انتهائها.

وبالرغم من المنافع الكبيرة التي أفرزتها تكنولوجيا المعلومات وشبكات المعلومات العالمية فإنها أيضا أوجدت خطراً حقيقياً³ تمثل بإمكانية جمع المعلومات وتخزينها والاتصال بها

1 راجع في ذلك : د/ محمد نصر القطري ، المسؤولية الجنائية لوسطاء تقديم خدمات شبكة الإنترنت ، بحث مقدم للمؤتمر الدولي العاشر حول "العصر الرقمي وإشكالياته القانونية " ، بكلية الحقوق، جامعة أسيوط في الفترة الممتدة من 5 إلي 6 /2016/4 ، ص 8 .

2 راجع في ذلك : الباحثة هبايش فوزية ، دور التجارة الإلكترونية في تفعيل مناطق التجارة الحرة حالة منطقة التجارة الحرة العربية الكبرى، رسالة ماجستير ، جامعة حسينية بن بوعلي بالشلف كلية العلوم الاقتصادية والتجارية وعلوم التسيير قسم العلوم الاقتصادية ، 2012 ، ص 15 وما بعدها .

3 راجع في ذلك : د/ أحمد عبد اللاه المراغي ، الجريمة الإلكترونية ودور القانون الجنائي في الحد منها ، دراسة تحليلية تأصيلية مقارنة ، بحث مقدم إلي المؤتمر العلمي العاشر لكلية الحقوق جامعة أسيوط ، "العصر الرقمي وإشكالياته القانونية " ، في الفترة من 5 - 6 أبريل 2016م ، ص 5 وما بعدها .

والوصول إليها، وجعلها متاحة علي الخط قابلة للاستخدام من قبل مختلف قطاعات الأعمال بدون علم أو معرفة صاحب المعلومات.

أنّ المواقع الرقمية التي يزورها المتصفح قادرة بدورها علي تحديد حركته فيها، وذلك من خلال إدخال ملفات في جهاز الكمبيوتر تعرف باسم «Cookies»¹. وبالإضافة إلي (Hard Disk) علي القرص الصلب صغيرة غالباً ما تتضمن ثغرات ، فإنّ المنتديات الرقمية ومواقع التواصل الاجتماعي، وأهمها «تويتر» و «فيسبوك» قد يتمكّن المتطفلين من الاطلاع علي أدق² التفاصيل الشخصية للمستخدمين فيها، وان كانت هذه المواقع تعمل باستمرار علي ابتكار سبل لحماية الخصوصية.

ففي البيئة الرقمية وعالم شبكات المعلومات العالمية ، يترك المستخدم آثار ودلالات كثيرة تتصل به بشكل سجلات رقمية حول الموقع الذي زاره والوقت الذي قضاه علي الشبكة والأمور التي بحث عنها والمواد التي قام بتنزيلها والوسائل التي أرسلها والخدمات والبضائع التي قام بطلبها وشرائها وكلها سجلات تتضمن تفاصيل دقيقة عن شخصية وحياة وهوايات وميول المستخدم علي الشبكة وهي سجلات مؤتمتة ذات محتوى شخصي يتصل بالفرد³. والتصفح والتجول عبر الإنترنت يترك لدي الموقع المزار كمية واسعة من المعلومات علي الرغم من ان جزءا من هذه المعلومات لازم لإتاحة الربط بالإنترنت والتصفح، وبمجرد الدخول إلي صفحة

1 راجع في ذلك :

– Osama ahmed Attalla، is the legal protection of digital privacy enough in Egypt’’? Protection of digital data privacy ،p5 .

2 راجع في ذلك : د/ جبالي أبو هشيمة كامل ، حماية البيانات الشخصية في البيئة الرقمية دراسة مقارنة ،

مرجع سابق ، ص9 وما بعدها .

3 راجع في ذلك :

– Osama ahmed Attalla، is the legal protection of digital privacy enough in Egypt’’? Protection of digital data privacy ”،p7

الموقع فان معلومات معينه تتوفر عن العميل وهي ما يعرف بمعلومات راس الصفحة (Header Information) ، وهذه المعلومات قد تتضمن:

1 (IP). عنوان بروتوكول الإنترنت العائد ومن خلاله يمكن تحديد اسم النطاق وتبعا له تحديد اسم الشركة للزبون او الجهة التي قامت بتسجيل النطاق عن طريق نظام أسماء المنظمات وتحديد موقعها.

2. المعلومات الأساسية عن المتصفح ونظام التشغيل وتجهيزات النظام المادية المستخدمة من قبل الزبون.

3. وقت وتاريخ زيارة الموقع.

4. مواقع الإنترنت وعنوان الصفحات السابقة التي زارها المستخدم قبل دخوله الصفحة في كل زيارة.

5. وقد تتضمن أيضا معلومات محرك البحث الذي استخدمه المستخدم للوصول الي الصفحة ، وتبعاً لنوع المتصفح قد يظهر عنوان البريد الرقمي للمستخدم.

6. وأيضاً تبعاً لتشغيل المستخدم أوامر خاصة حول إدارة التعامل مع الشبكة قد تظهر معلومات حول الوقت الذي تم قضاؤه في كل صفحة وبيان المعلومات التي أرسلت واستقبلت.

فعندما يستخدم الأفراد مواقع الإنترنت فإنهم يتوقعون قدرا من الخفية في نشاطهم أكثر مما يتوقعون في العالم المادي الواقعي ، ففي الأخير يمكن ملاحظة وجودهم ومراقبتهم من قبل الآخرين ، وما لم يكشف الشخص عن بيانات تخصه فإنه يعتقد أن أحدا لن يعرف من هو او ماذا يفعل ، لكن الإنترنت عبر نظم الخوادم ونظم إدارة الشبكات تصنع قدرا كبيرا من المعلومات

عند كل وقفة في فضاء الشبكة . وهذه البيانات قد يتم اصطيادها¹ ومعرفتها عن موظفي منشأة ما مثلا - من قبل صاحب العمل عند استخدامه للشبكة او لاشتراكاتهم المربوطة عليها ، وقد تجمع من قبل المواقع المزاره نفسها، وكما قلنا فان جمع شتات معلومات وسلوكيات معينة قد يقدم أوضح صورة عن شخص لم يرد كشف أي من تفاصيل لم يرد الكشف عنها².

1 راجع في ذلك : راجع في ذلك : أم.د.مني تركي و م.م. جان سيريل ، الخصوصية المعلوماتية وأهميتها ومخاطر التقنيات ، مرجع سابق ، ص9 وما بعدها .

2 راجع في ذلك : الباحث / حسين خلف موسي، استراتيجية أمن المعلومات في ظل حروب الجيل السادس ، خاص لمركز شُرُفات لدراسات العولمة والإرهاب ، عمان ،الأردن 9 مارس، 2017 ، ص 10 وما بعدها .

المطلب الثالث

التحديات التي تواجه أنظمة أمن المعلومات واستراتيجياتها والحماية القانونية

تواجه أنظمة المعلومات بعض المشكلات الشائعة التي بدأت تغزو أنظمة المعلومات و تساهم في تدميرها أو تخريبها أو سرقة المعلومات المحفوظ في أجهزة الحاسوب او الموجودة علي الشبكة والتي من ابرزها و أهمها ما سنعرض له لاحقا على النحو التالي :

الفرع الأول: التحديات التي تواجه أنظمة أمن المعلومات

الفرع الثاني : إستراتيجيات أمن المعلومات Security Policy

الفرع الثالث : الحماية القانونية لأمن المعلومات

الفرع الأول

التحديات التي تواجه أنظمة أمن المعلومات

اولا : خرق الحماية المادية **Physical security Breaches of**¹

1. **التفتيش في مخلفات التقنية Dumpster diving** : ويقصد به قيام المهاجم بالبحث في مخلفات المؤسسة من القمامة والمواد المتروكة بحثا عن أي شيء يساعده علي إختراق النظام ، كالأوراق المدون عليها كلمات السر ، او مخرجات الكمبيوتر التي قد تتضمن معلومات مفيدة ، او الأقراص الصلبة المرمية بعد استبدالها ، او غير ذلك من المواد المكتوبة او الملاحظات او أي أمر يستدل منه علي أية معلومة تساهم في الاختراق . وحتى ندرك مخاطر النفايات الرقمية² ، فقد حصل أن بيعت من قبل وزارة العدل الأمريكية مخلفات أجهزة تقنية بعد أن تقرر إتلافها ، وكان من ضمنها نظام كمبيوتر يحتوي قرصه الصلب علي كافة العناوين الخاصة ببرنامج حماية الشهود ، وبالرغم من إنه لم يتم فعليا استثمار هذه المعلومات ، إلا أن مخاطر كشف هذه العناوين استدعي إعادة نقل كافة الشهود وتغيير مواطن إقامتهم وهوياتهم وهو ما تطلب ميزانية ضخمة لا لشيء إلا للإخفاق في التخلص الأمن من النفايات الرقمية .

2. **الالتقاط السلكي Wiretapping** :- والمقصود هنا ببساطة التوصل السلكي المادي مع الشبكة او توصيلات النظام لجهة استراق السمع او سرقة والاستيلاء علي المعطيات

1 راجع في ذلك : الباحث / حسين خلف موسي ، استراتيجية أمن المعلومات في ظل حروب الجيل السادس ، مرجع سابق ، ص16 وما بعدها .

2 راجع في ذلك : المحامي/يونس عرب ، أمن المعلومات ماهيتها وعناصرها واستراتيجياتها ، مرجع السابق ، ص16 .

المتبادلة عبر الأسلاك ، وهي أنشطة تتم بطرق سهلة او معقدة تبعا لنوع الشبكة وطرق

التوصل المادي فيما يعرف " بالإيداع الرقمي " او " الإيداع الرقمي " ¹.

3. استراق الأمواج Eavesdropping on Emanations : ويتم ذلك باستخدام لواقط تقنية

لتجميع الموجات المنبعثة من النظم باختلاف أنواعها كالتقاط موجات شاشات الكمبيوتر

الضوئية او التقاط الموجات الصوتية من أجهزة الاتصال .

4. أنكار او إلغاء الخدمة Denial or Degradation of Service : والمقصود هنا الإضرار

المادي بالنظام لمنع تقديم الخدمة ، كضخ الرسائل البريدية الرقمية دفعة واحدة لتعطيل

النظام .

ثانيا :خرق الحماية المتعلقة بالأشخاص وشؤون الموظفين Personnel

security Breaches of

تعد المخاطر المتصلة بالأشخاص والموظفين ، وتحديد المخاطر الداخلية منها ، واحدة

من مناطق الاهتمام العالي لدي جهات أمن المعلومات ، اذ ثمة فرصة لان يحقق أشخاص من

الداخل ما لا يمكن نظريا ان يحققه أحد من الخارج ، وتظل أيضا مشكلة صعوبات كشف هؤلاء

قائمة ان لم يكن ثمة نظام أداء وصلاحيات يتيح ذلك ، وبالعوم ثمة مسميات وطوائف عديدة

لهذه المخاطر نتناول فيما بعد أبرزها².

1 راجع في ذلك : د/ معتز السيد الزهيري ، المواجهة الجنائية لجرائم الإيداع الإلكتروني ، بحث منشور بمؤتمر

القانون والتكنولوجيا ، كلية الحقوق ، جامعة عين شمس ، ديسمبر 2017 ، ص 113 وما بعدها.

2 راجع في ذلك : الباحث / حسين خلف موسي ، استراتيجية أمن المعلومات في ظل حروب الجيل السادس ،

مرجع سابق ، ص 16 وما بعدها ، وراجع أيضا: المحامي/ يونس عرب، أمن المعلومات ماهيتها وعناصرها

واستراتيجياتها ، مرجع السابق ، ص 16 وما بعدها .

1. **التخفي بأنتحال صلاحيات شخص مفوض Masquerading**: والمقصود هنا الدخول إلي النظام عبر استخدام وسائل التعريف العائدة لمستخدم مخول بهذا الاستخدام ، لاستغلال كلمة سر أحد المستخدمين واسم هذا المستخدم ، او عبر استغلال نطاق صلاحيات المستخدم الأصلي ومع أن هذا النمط من الاختراقات هو الشائع سواء في البيئة الداخلية للمنشأة او الخارجية ، إلا أن وضعه ضمن طائفة الاختراقات المتصلة بالموظفين ومستخدمي النظام من الداخل مصدره حصوله الغالب في هذه البيئة بسبب أخطاء تشارك الموظفين كلمات السر ووسائل التعريف ، وبسبب إمكان الحصول عليها عن طريق استراق النظر او نحو ذلك من الأساليب التي تتواجد في بيئة العمل الداخلي وتتيح الحصول علي كلمات المرور او وسائل التعريف¹.

2. **الهندسة الاجتماعية Social Engineering** : ويصنف هذا الأسلوب ضمن الحماية المادية أحيانا ويرجع إلي أنشطة الحصول علي معلومات تهيئ الاقتحام من خلال علاقات اجتماعية وذلك باستغلال الشخص أحد عناصر النظام - أشخاصه - بإيهامه باي أمر يؤدي إلي حصول هذا الشخص علي كلمة مرور او علي أية معلومة تساعد في تحقيق اعتدائه ، وابطس مثال أن يتصل شخص بأحد العاملين ويطلب منه كلمة سر النظام تحت زعم إنه من قسم الصيانة او قسم التطوير او غير ذلك ، ولطبيعة الأسلوب الشخصي في الحصول علي معلومة الاختراق او الاعتداء سميت الهندسة الاجتماعية .

3. **الإزعاج والتحرش Harassment** :- وهي تهديدات يندرج تحتها أشكال عديدة من الاعتداءات والأساليب ، ويجمعها توجيه رسائل الإزعاج والتحرش وربما التهديد والابتزاز او في أحيان كثيرة رسائل المزاح علي نحو يحدث مضايقة وإزعاجا بالغيث ، وليست حكرا علي

1 راجع في ذلك : الباحث / حسين خلف موسي ، استراتيجية أمن المعلومات في ظل حروب الجيل السادس ، مرجع سابق ، ص16 وما بعدها.

البريد الرقمي بل تستغل مجموعات الحوار والأخبار والنشرات الرقمية في بيئة الإنترنت ، كما إنها ليست حكرًا علي بيئة الموظفين والمستخدمين ، بل هي نمط متواجد في مختلف التفاعلات عبر الشبكة وعبر البريد الرقمي ، والصحيح إنها شائعة كاعتداءات من الخارج وغالبًا ما تكون مشكلة تتصل بالأشخاص أكثر منها بمؤسسات الأعمال ، ومن هنا يصنفها أصحاب هذا التصنيف ضمن هذه الطائفة¹.

4. **قرصنة البرمجيات Software Piracy** : وقرصنة البرامج تتحقق عن طريق نسخها دون تصريح أو استغلالها علي نحو مادي دون إذن بهذا الاستغلال ، أو تقليدها ومحاكاتها والانتفاع المادي بها علي نحو يخل بحقوق المؤلف ، وهو نشاط يندرج في حقيقته ضمن طائفة الاعتداءات والمخاطر التي تستهدف البرمجيات عموماً ، وهو قطاع استقل بذاته من بين قطاعات جرائم الكمبيوتر².

ثالثاً : خرق الحماية المتصلة بالاتصالات والمعطيات Communications

Breaches of Security and

- 1 راجع في ذلك : د / معتز السيد الزهري ، بحث بعنوان " الإيذاء عبر مواقع التواصل الاجتماعي Cyber bullying " ، بحث منشور بالمؤتمر العلمي الدولي الثاني "المجتمع العربي وشبكات التواصل الاجتماعي في عالم متغير" ، 31 أكتوبر - 2 نوفمبر 2017 ، جامعة السلطان قابوس، مسقط، سلطنة عمان ، ص4 وما بعدها ، وراجع أيضا : د/ معتز السيد الزهيري، المواجهة الجنائية لجرائم الإيذاء الإلكتروني ، مرجع سابق ، ص119 وما بعدها
- 2 راجع في ذلك : الباحث / حسين خلف موسي ، استراتيجية أمن المعلومات في ظل حروب الجيل السادس ، مرجع سابق ، ص18 وما بعدها.
- 3 راجع في ذلك: المحامي/ يونس عرب ، أمن المعلومات ماهيتها وعناصرها واستراتيجياتها ، مرجع السابق ، ص17 وما بعدها .

والمقصود بهذه الطائفة الأنشطة التي تستهدف المعطيات والبرمجيات ذاتها وتشمل

طائفتين:

▪ هجمات المعطيات : Data Attacks

- النسخ غير المصرح به للمعطيات Unauthorized Copying of Data:-

وهي العملية الشائعة التي تستتبع الدخول غير المصرح به للنظام ، حيث يمكن الاستيلاء عن طريق النسخ لكافة أنواع المعطيات ، والتي تشمل البيانات والمعلومات والأوامر والبرمجيات وغيرها.

- تحليل الاتصالات Traffic Analysis :- الفكرة هنا ببساطة إن الهجوم ينصب

علي دراسة أداء النظام في مرحلة التعامل ومتابعة ما يتم فيه من اتصالات وارتباطات بحيث يستفاد منها في تحديد مسلكيات المستخدمين وتحديد نقاط الضعف ووقت الهجوم المناسب وغير ذلك من مسائل يجمعها فكرة الرقابة علي حركة النظام بغرض تيسير الهجوم عليه .

- القنوات المخفية Covert Channels :- وهي عمليا صورة من صور اعتداءات

التخزين ، حيث يخفي المقتحم معطيات او برمجيات او معلومات مستولي عليها كأرقام بطاقات ائتمان في موضع معين من النظام ، وتتعدد أغراض الإخفاء، فقد تكون تمهيدا لهجوم لاحق او تغطية اقتحام سابق او مجرد تخزين لمعطيات غير مشروعة .

▪ هجمات البرمجيات: Software Attacks¹:

1 راجع في ذلك : الباحث / حسين خلف موسي ، استراتيجية أمن المعلومات في ظل حروب الجيل السادس ، مرجع سابق ، ص19 وما بعدها .

- **الأبواب الخلفية Trap Doors** : الأبواب الخلفية ثغرة او منفذ في برنامج يتيح للمخترق الوصول من خلاله إلي النظام ، إنه ببساطة مدخل مفتوح تماما كالباب الخلفي للمنزل الذي ينفذ منه السارق.
- **السرقه او اختلاس المعلومة او الاستخدام اللحظي (سرقة او اختطاف الجلسات Session Hijacking)** :- وليس المقصود هنا أنشطة الاستيلاء علي البيانات عبر واحد او أكثر من الأساليب التقنية المتقدمة او اللاحقة ، إنما المقصود إن يستغل الشخص استخداما مشروعا من قبل غيره لنظام ما ، فيسترق النظر او يستخدم النظام عندما تتاح له الفرصة لانشغال المستخدم دون علمه ، او إن يجلس ببساطة مكان مستخدم النظام فيطلع علي المعلومات او يجري أية عملية في النظام ، وذلك بقصد الاستيلاء علي بيانات او الحصول علي معلومات تستخدم في اختراق او اعتداء لاحق او لتنفيذ نشاط تدميري آني او لكشف معطيات بشكل فوري .
- **الهجمات عبر التلاعب بنقل المعطيات عبر انفاق النقل Tunneling** : انفاق النقل في الأصل طريقة تقنية مشروعة لنقل المعطيات عبر الشبكات غير المتوافقة، لكنها تصبح طريقة اعتداء عندما تستخدم حزم المعطيات المشروعة لنقل معطيات غير مشروعة.
- **الهجمات الوقتية Timing attacks** وهي هجمات تتم بطرق تقنية معقدة للوصول غير المصرح به إلي البرامج او المعطيات ، وتقوم جميعها علي فكرة استغلال وقت تنفيذ الهجمة متزامنا مع فواصل الوقت التي تفصل العمليات المرتبة في النظام ، وتضم في نطاقها العديد من الأساليب التقنية لتنفيذ الهجوم ، منها إساءة استغلال الأوضاع او الأنماط

العادية للأداء والكيفية في النظام Race conditions والهجمات غير المتزامنة أو غير المتوافقة المتصلة باستغلال ترتيب تنفيذ العمليات الاعتيادية Asynchronous attacks¹.

- البرمجيات الخبيثة Malicious Code كالفايروسات Viruses وحصان طروادة Trojan Horses والدودة الرقمية Worms والسلامي Salamis والقنابل المنطقية Logic Bombs.... الخ :- الجامع المشترك بين هذه البرمجيات إنها برمجيات ضارة تستغل للتدمير سواء تدمير النظام أو البرمجيات أو المعطيات أو الملفات أو الوظائف أو تستثمر للقيام بمهام غير مشروعة كإنجاز احتيال أو غش في النظام ، والحقيقة إنها ليست تسميات مترادفة للفيروسات الشائعة ، إنها تختلف عن بعضها البعض من حيث تركيبها أحيانا وأحيانا من حيث طريقة أحداث النتيجة وأحيانا أسلوبها في الهجوم².

والفيروسات تمثل حرب الهجمات القائمة والشائعة الآن بسبب استغلال سوء استخدام شبكة الإنترنت وتوفيرها فرصة نشر البرمجيات الضارة حول العالم ، ولم تعد مجرد هجمة تستهدف نظاما بعينه أو تلحق ضررا بأحد الملفات ، بل عدت هجمات منظمة تلحق خسائر بالملايين ، ومن باب التمثيل لا أكثر ، فإن هجمات الفايروسات وما الحقته من خسائر قد لا يتصور البعض حجمها ، فإذا كان الفيروس الذي أطلقه موريس عام 1988 وضرب نحو 6000 كمبيوتر عبر انتشاره إليها من خلال شبكة الإنترنت ، فهذا الفايروس الذي تشير أحدث التقارير

1 راجع في ذلك : المحامي/ يونس عرب، أمن المعلومات ماهيتها وعناصرها واستراتيجياتها ، مرجع السابق ، ص19 وما بعدها.

2 راجع في ذلك : المحامي يونس عرب ، جرائم الكمبيوتر والإنترنت إيجاز في المفهوم والنطاق والخصائص والصور والقواعد الإجرائية للملاحقة والإثبات ، ورقة عمل مقدمة الي مؤتمر الأمن العربي 2002 ، تنظيم المركز العربي للدراسات والبحوث الجنائية ، أبو ظبي 10-12/ 2002/2 ، ص2 وما بعدها .

أن مصدره الصين ، الحق خسائر أوليه قدرت بما يزيد عن 2.5 مليار ولا يزال يهدد غالبية نظم الكمبيوتر والشبكات حول العالم¹.

رابعا : الهجمات والمخاطر المتصلة بعمليات الحماية Breaches Of

Operations Security

وإذا ما اردنا ان نوصف المخاطر المتصلة بعمليات الحماية ذاتها ربما نكون في الحقيقة أمام كافة أنواع المخاطر والهجمات والاعتداءات ، لكن من زاوية تقنية ضيقة ، يشار إلي خمسة أنواع من الأساليب ضمن هذه الطائفة ، بعضها يتصل بالهجمات التي تستهدف نظام او إستراتيجية الدخول ، وبعضها يستهدف نظام إدخال ومعالجة والبيانات ، وبعضها يصنف كفعل أولي لتحقيق عمليات الدخول غير المصرح به إلي مختلف أنواع الشبكات ، وسنشير بإيجاز إلي هذه الأساليب والاعتداءات ، مع إيضاح لمسميات آخري من الأنشطة والأساليب والاعتداءات تتصل باختراق الشبكات تحديدا وبيان لأهم نقاط الضعف وفقا لما توصلت إليه أدلة أمن المعلومات المتخصصة نتيجة العديد من الدراسات البحثية² :

1. العبث (الغش) بالبيانات Data Diddling :- ويستهدف هذا الهجوم او الاعتداء تغيير البيانات او إنشاء بيانات وهمية في مراحل الإدخال او الاستخراج ، ويتم في الحقيقة بعشرات الأنماط والأساليب التقنية .

1 راجع في ذلك : الباحث / حسين خلف موسي ، استراتيجية أمن المعلومات في ظل حروب الجيل السادس ، مرجع سابق ، ص20.

2 راجع في ذلك : المحامي/ يونس عرب، أمن المعلومات ماهيتها وعناصرها واستراتيجياتها ، مرجع السابق ، ص20 وما بعدها.

2. **خداع بروتوكول الإنترنت IP Spoofing (التخفي باستغلال بروتوكولات النقل):** الحقيقة أن اصطلاح Spoofing لا يعني التخفي ، فهو اصطلاح يتعلق بالغش والخداع والإيهام والتقليد والمحاكاة والسخرية ، لكن استخدامه الشائع الآن يتعلق بهجمات فايروسات الإنترنت ، والفكرة هنا قريبة من فكرة التخفي التي عرضنا لها أعلاه عندما يتخذ شخص او ينتحل صفة مستخدم آخر مخول بالاستخدام ، لكن الفرق هنا ، أننا نتحدث عن وسيلة تقنية بحتة ، بحيث يقوم المهاجم عبر هذه الوسيلة بتزوير العنوان المرفق مع حزمة البيانات المرسله ، بحيث يظهر للنظام - طبعا المعتمد في تبادل المعطيات علي بروتوكولات النقل واهمها هنا بروتوكول الإنترنت الأساسي - علي إنه عنوان صحيح مرسل من داخل الشبكة ، بحيث يسمح النظام لحزمة البيانات بالمرور باعتبارها حزمة مشروعة (أن جاز التعبير). " ضرب الكراك او استخدام برامج لتحميل السيريال نمبر بدون مقابل " وهو ما يعد مخالف لحقوق الملكية الفكرية¹.

3. - **تشتم كلمات السر (جمعها والتقاطها) Password Sniffing :** وإذا كانت أنشطة الاعتداء التي تتم باستعمال كلمات السر كانت تتم غالبا فيما سبق عن طريق تخمين كلمات السر مستفيدة من ضعف الكلمات عموما وشيوع اختيار الأفراد لكلمات سهلة تتصل بمحيطهم الأسري او محيط العمل او حياتهم الشخصية ، فان الجديد استخدام برمجيات يمكنها تشتم او التقاط كلمات السر خلال تجوالها في جزء من الشبكة او أحد عناصرها ومراقبتها ومتابعتها لحركة الاتصال علي الشبكة ، بحيث يقوم هذا البرنامج من حيث الأصل بجمع أول 128 بايت او أكثر - مثلا - من كل اتصال بالشبكة التي تجري مراقبتها وتتبع

1 راجع في ذلك : د/ حسن جمعي ، مدخل إلي حقوق الملكية الفكرية ، ندوة الويبو الوطنية عن الملكية الفكرية للصحفيين ووسائل الإعلام ، المنظمة العالمية للملكية الفكرية (الويبو) ، بالتعاون مع وزارة الإعلام المنامة، 16 يونيوه/حزيران 2004 ، ص4 وما بعدها .

حركة الاتصال عليها¹، وعندما يطبع المستخدم كلمة السر او اسم المستخدم ، فان البرنامج يجمع هذه المعلومات وينسخها إضافة إلي أن أنواع من هذه البرامج تجمع المعلومات الجزئية وتعيد تحليلها وربطها معا كما تقوم بعضها بإخفاء أنشطة الالتقاط بعد قيامها بمهمتها

4. - **المسح والنسخ Scanning**²: وهو أسلوب يستخدم فيه برنامج (الماسح - ware dialer او demon dialer processes) الذي هو برنامج احتمالات يقوم علي فكرة تغيير التركيب او تبديل احتمالات المعلومة ، ويستخدم تحديدا بشأن احتمالات كلمة السر او رقم هاتف الموديم او نحو ذلك ، وابسط نمط فيه عندما تستخدم قائمة الاحتمالات لتغيير رقم الهاتف بمسح قائمة أرقام كبيرة للوصول إلي احدها الذي يستخدم موديم للاتصال بالإنترنت ، او إجراء مسح لاحتمالات عديدة لكلمة سر للوصول إلي الكلمة الصحيحة التي تمكن المخترق من الدخول لنظام ، ومن جديد فان هذا أسلوب تقني يعتمد واسطة تقنية هي برنامج (الماسح) بدلا من الاعتماد علي التخمين البشري .

5. - **هجمات استغلال المزايا الإضافية Excess Privileges**³ : الفكرة هنا تتصل بواحد من اهم استراتيجيات الحماية ، فالأصل أن مستخدم النظام - تحديدا داخل المؤسسة - محدد له نطاق الاستخدام ونطاق الصلاحيات بالنسبة للنظام ، لكن ما يحدث في الواقع

1 راجع في ذلك :

Yamaguchi (Atsushi): "Computer crimes and others crimes against information Technology in Japan, Rev. int. de dr. pén. 1993. P 448

2 راجع في ذلك : الباحث / حسين خلف موسي ، استراتيجية أمن المعلومات في ظل حروب الجيل السادس ، مرجع سابق ، ص 21 .

3 راجع في ذلك : المحامي/ يونس عرب ، أمن المعلومات ماهيتها وعناصرها واستراتيجياتها ، مرجع السابق ، ص 20 .

العملي أن مزايا الاستخدام يجري زيادتها دون تقدير لمخاطر ذلك او دون علم من الشخص نفسه إنه يحظى بمزايا تتجاوز اختصاصه ورغباته ، في هذه الحالة فان أي مخترق للنظام لن يكون فقط قادرا علي تدمير أو التلاعب ببيانات المستخدم الذي دخل علي النظام من خلال اشتراكه او عبر نقطة الدخول الخاصة به ، إنه ببساطة سيتمكن من تدمير مختلف ملفات النظام حتي غير المتصلة بالمدخل الذي دخل منه لأنه استثمر المزايا الإضافية التي يتمتع بها المستخدم الذي تم الدخول عبر مدخله . وأوضح مثال علي هذا الخطر في العالم المادي ، تمكن شخص من دخول غرفة مدير فندق مثلا بقصد سرقة فيجده في غرفته مفاتيح كافة قاصات الأمانات او مفاتيح الماستر الذي يفتح غرف الفندق جميعها . وهذا وحده يعطينا التصور لأهمية إستراتيجية أمن المعلومات في الهيئات والمؤسسات فتحديد الامتيازات والصلاحيات قد يمنع في حقيقته من حصول دمار شامل ويجعل الاختراقات غير ذي اثر ، ولن تسمح الإستراتيجية الواعية للقول أن المستخدم الغلاني لديه مزايا لا يعرف عنها بل لن تسمح بوجودها أصلا.

خامسا : المخاطر التي تهدد أمن المعلومات

و هذه المخاطر ما يلي¹:

1 - اختراق الأنظمة : ويتحقق ذلك بدخول شخص غير مخول بذلك إلي نظام الكمبيوتر والقيام بأنشطة غير مصرح له بها كتعديل البرمجيات التطبيقية وسرقة البيانات السرية او تدمير الملفات او البرمجيات او النظام او لمجرد الاستخدام غير المشروع . ويتحقق الاقتحام بشكل تقليدي من خلال أنشطة (التنقيب والتخفي) ويراد به تظاهر الشخص المخترق بأنه شخص آخر

1 راجع في ذلك : الباحث / حسين خلف موسي ، استراتيجية أمن المعلومات في ظل حروب الجيل السادس ، مرجع سابق ، ص 22 وما بعدها .

مصرح له بالدخول . او من خلال استغلال نقاط الضعف في النظام كتجاوز إجراءات السيطرة والحماية او من خلال المعلومات التي يجمعها الشخص المخترق من مصادر مادية او معنوية ، كالالتقيب في قمامة الهيئات والمؤسسات للحصول علي كلمات السر او معلومات عن النظام او عن طريق الهندسة الاجتماعية كدخول الشخص إلي مواقع معلومات حساسة¹ داخل النظام ككلمات السر او المكالمات الهاتفية .

2 - الاعتداء علي حق الإذن : ويتم من خلال قيام الشخص المخول له استخدام النظام

لغرض ما باستخدامه في غير هذا الغرض دون أن يحصل علي الإذن بذلك ، وهذا الخطر يعد من الأخطار الداخلية في حقل إساءة استخدام النظام من قبل موظفي الهيئات والمؤسسات ، وهو قد يكون أيضا من الأخطار الخارجية ، كاستخدام المخترق حساب شخص مخول له باستخدام النظام عن طريق تخمين كلمة السر الخاصة به او استغلال نقطة ضعف بالنظام للدخول إليه بطريق مشروع او من جزء مشروع ومن ثم القيام بأنشطة غير مشروعة .

3 - زراعة نقاط الضعف : عادة ينتج هذا الخطر عن اقتحام من قبل شخص غير

مصرح له بذلك او من خلال مستخدم مشروع تجاوز حدود الإذن الممنوح له بحيث يقوم الشخص بزرع مدخل ما يحقق له الاختراق فيما بعد . ومن أشهر امثله زراعة المخاطر حضان طروادة ، وهو عبارة عن برنامج يؤدي غرضا مشروعا في الظاهر لكنه يمكن ان يستخدم في الخفاء للقيام بنشاط غير مشروع ، كأن يستخدم برنامج معالجة كلمات ظاهريا لتحرير وتنسيق النصوص في

1 حدد المشرع قانون رقم ١٥١ لسنة ٢٠٢٠ بإصدار قانون حماية البيانات الشخصية ، إجراءات إتاحة البيانات الشخصية ، و البيانات الشخصية الحساسة بالمواد من (10-13) .

حين يكون غرضه الحقيقي طباعة كافة ملفات النظام ونقلها إلي ملف مخفي بحيث يمكن للمخترق أن يقوم بطباعة هذا الملف والحصول علي محتويات النظام .

4 - مراقبة الاتصالات : بدون اختراق كمبيوتر المجني عليه يتمكن الجاني من الحصول علي معلومات سرية غالبا ما تكون من المعلومات التي تسهل له مستقبلا اختراق النظام وذلك ببساطة من خلال مراقبة الاتصالات من إحدى نقاط الاتصال او حلقاتها .

5 - اعتراض الاتصالات¹ : وكذلك بدون اختراق النظام يقوم الجاني في هذه الحالة باعتراض المعطيات المنقولة خلال عملية نقل البيانات ويجري عليها التعديلات والمعالجات التي تتناسب مع غرض الاعتداء ويشمل اعتراض الاتصالات قيام الجاني بخلق نظام وسيط وهمي بحيث يكون علي المستخدم أن يمر من خلاله ويزود النظام بمعلومات حساسة بشكل طوعي .

6 - إنكار الخدمة : ويتم ذلك من خلال القيام بأنشطة تمنع المستخدم الأساسي من الوصول إلي المعلومات او الحصول علي الخدمة وأبرز أنماط إنكار الخدمة إرسال كمية كبيرة من رسائل البريد الرقمي دفعة واحدة إلي موقع معين بهدف إسقاط النظام المستقبل لعدم قدرته علي احتمالها او توجيه عدد كبير من عناوين الإنترنت علي نحو لا يتيح عملية تجزئة حزم المواد المرسله فتؤدي إلي اكتظاظ الخادم وعدم قدرته علي التعامل معه .

1 هذا ولقد تنبه المشرع المصري لجرائم امن المعلومات فعاقب وجرم بقانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات جرائم امن المعلومات علي النحو التالي : جريمة الانتقاع بدون وجه حق بخدمات الاتصالات والمعلومات وتقنياتها (م13) ، جريمة تجاوز حدود الحق في الدخول (م14) ، جريمة الدخول غير المشروع (م15) ، جريمة الاعتراض غير المشروع (م16) ، جريمة الاعتداء علي سلامة البيانات والمعلومات والنظم المعلوماتية (م17) ، جريمة الاعتداء علي البريد الإلكتروني أو المواقع أو الحسابات الخاصة (م18) ، جريمة الاعتداء علي تصميم موقع (م19) ، جريمة الاعتداء علي الأنظمة المعلوماتية الخاصة بالدولة (م20) ، جريمة الاعتداء علي سلامة الشبكة المعلوماتية (م21) .

7 - عدم الإقرار بالقيام بالتصرف : ويتمثل هذا الخطر في عدم إقرار الشخص المرسل

إليه او المرسل بالتصرف الذي صدر عنه ، كأن ينكر إنه ليس هو شخصيا الذي قام بإرسال

طلب الشراء عبر الإنترنت .

الفرع الثاني

إستراتيجيات أمن المعلومات Security Policy

تتعلق الإستراتيجية الفاعلة من القدرة علي إيجاد نظام متواصل لعملية تحليل المخاطر وتحديد احتياجات الحماية لحظة بلحظة ، وعملية تحليل المخاطر هي في حقيقتها نظام متكامل للتحليل وسلامة التصرف تبدأ من الإعداد الجيد القائم علي فهم وإدراك وتحديد عناصر النظام والعمليات والمخاطر ، ومن ثم تحديد معايير التهديد ونطاق الحماية المطلوب منها وتبعاً له وسائل الحماية ، لتنتهي ببيان معيار الخسارة المقبولة التي يتصور تحققها بغض النظر عن مستوى الحماية ومستوي ودرجة الاستعداد للمواجهة¹.

وبناء علي ما سبق يمكن تعريف إستراتيجية أمن المعلومات ، او سياسة أمن المعلومات بأنها مجموعة القواعد التي يطبقها الأشخاص عند التعامل مع التقنية ومع المعلومات داخل الهيئات والمؤسسات وتتصل بشؤون الدخول إلي المعلومات والعمل علي معالجتها وإدارتها .

اولا : التعريف بوسائل الأمن التقنية

ان ما نتحدث عنه هنا ليس تحديدا لمنتجات الأمن التي لا يمر لحظة دون وجود منتج جديد ، ولا يمر يوم أيضا دون إعادة تقييم لوسائل الأمن ، وهي وسائل ومنتجات تتوزع بين الوسائل المادية للحماية وبرمجيات وحلول الحماية ، ونظريات وبروتوكولات الحماية ، ولا نبالغ

1 راجع في ذلك : الباحث / حسين خلف موسي ، استراتيجية أمن المعلومات في ظل حروب الجيل السادس ، مرجع سابق ، ص 25 وما بعدها .

ان قلنا أن سوق وسائل الأمن اصبح يتقدم في عدد منتجاته علي سوق الأجهزة ذاتها والحلول ، لان كل منتج وكل برنامج جديد يتطلب قدرا معيناً من وسائل الحماية الفنية

كما إن هذا الدليل لا يقيم وسائل الأمن القائمة ، فيتحدث مثلا عن مدي فعالية الجدران النارية او مدي مقدرة الشبكات الخاصة الافتراضية علي توفير الأمن والثقة ، إنما يعرض فقط للشائع من طوائف وسائل أمن المعلومات بوجه عام والتي تندرج في نطاق كل طائفة منها آلاف الوسائل التي تتباين تبعا للاحتياجات وتبعا لطبيعة محل الحماية .

الخطأ السائد يكمن في الاعتقاد أن نظم الكمبيوتر والشبكات تتشابه من حيث احتياجاتها الأمنية، إذ حتي في نطاق الطائفة الواحدة من أنظمة الكمبيوتر التي تستخدم نفس برمجيات التشغيل او تعتمد نفس وسائل الربط وحلول الشبكات وتجهيزاتها ، نجد اختلافا في متطلبات الحماية لما يزل قائما ومرد لك التباين بين طبيعة العمليات التي يقوم بها النظام والتباين بين طبيعة المعطيات نفسها ، والتباين بين وسائل الاستخدام والمستخدمين ، وأخيرا ، التباين في درجة التوازن المطلوبة ما بين إجراءات الأمن وأداء وفعالية النظام نفسه¹ .

إن بناء وسائل أمن فاعلة يتطلب الانطلاق من احتياجات المؤسسة الخاصة وأغراض الأمن فيها ، ويقوم – كما سبق وأوضحنا وكما سنوضح تاليا في البند 1-5 ، علي ادراك الاحتياجات الداخلية فما نحمله يختلف عما يحمله غيرنا ، ومصادر الخطر التي تواجه مؤسسة مالية مثلا تختلف عن المخاطر التي تواجه مؤسسة عسكرية او تواجه نظام كمبيوتر مستخدم فرد

1 راجع في ذلك : المحامي/ يونس عرب، أمن المعلومات ماهيتها وعناصرها واستراتيجياتها ، مرجع السابق ، ص38 وما بعدها .

. واحتياجات حماية جهاز الكمبيوتر وبرمجياته والمعطيات المخزنة فيه يتخلف عن احتياجات حماية شبكة داخلية او حماية الارتباط بشبكة عالمية¹.

ولهذا فان تقنيات الحماية مرتبطة بعامل الاحتياجات الخاصة المعتمدة علي تقدير قائم علي ركائز وحقائق سليمة ، ويعتمد أيضا علي التوازن بين متطلبات الحماية وسرعة الأداء ، والتوازن أيضا بين متطلبات الحماية والميزانية المرصودة لتوظيف وسائل الأمن . ومنطق استخدام تقنيات إحدى الشركات لمجرد أنها عالمية او مميزة ، منطق لا يتفق مع إستراتيجية الأمن ذاته ، ولا نبالغ إن قلنا إن مئات المؤسسات - وتحديا المالية - استخدمت حزما من التقنيات في ضمنها مثلا جدران نارية وبرمجيات تشفير - كانت فاعلة في حالات أخرى - لم تكن لتحل مشكلاتها الأمنية ، وفي الوقت ذاته اذا تمكنت من حلها فإنها أحدثت أثرا سلبيا علي كفاءة الأداء وفعالية النظام .

إن سوق الوسائل التقنية في مرحلة ما كان مجرد منتجات وخدمات مضافة الي طائفة منتجات وخدمات شركات تقنية المعلومات المختلفة وغالبا ما تكون وسائل في خدمة بقية منتجاتها وخدماتها ومع إن شركات تقنيات المعلومات لما تنزل في غالبيتها تخصص وحدات من بين وحدات نشاطها لوسائل الأمن فان سوق تقنية المعلومات انتقل الي التخصصية ، فنشأت شركات عملاقة تعمل في حقل أمن المعلومات ، ووسائله وحلوله ، واتجهت الدراسات البحثية والاستراتيجية والعلمية وحتى القانونية الي التعامل مع وسائل الأمن علي استقلال ، فثمة أدلة ودراسات شاملة في ميدان الفايروسات ووسائل مكافحتها وثمة مثلها في ميدان التشفير وحلوله ، وأخري في ميدان وسائل التعريف والتحكم في الدخول الي النظام ، وهكذا.

1 راجع في ذلك : الباحث / صغير يوسف ، الجريمة المرتكبة عبر الإنترنت ، رسالة ماجستير ، كلية الحقوق والعلوم السياسية ، جامعة مولود معمري تيزي وزو ، 2013 ، ص 92 وما بعدها

1. وسائل الأمن الشائعة¹ :

وسائل أمن المعلومات هي مجموعة من الآليات والإجراءات والأدوات والمنتجات التي تستخدم للوقاية من أو تقليل المخاطر والتهديدات التي تتعرض لها الكمبيوترات والشبكات وبالعموم نظم المعلومات وقواعدها.

و بشكل أساسي تصنف وسائل الأمن في ضوء غرض الحماية الي الطوائف

التالية :

-مجموعة وسائل الأمن المتعلقة بالتعريف بشخص المستخدم وموثوقية الاستخدام ومشروعيته Identification and authentication ، وهي الوسائل التي تهدف الي ضمان استخدام النظام او الشبكة من قبل الشخص المخول بهذا الاستخدام ، وتضم هذه الطائفة كلمات السر بأنواعها ، والبطاقات الذكية المستخدمة للتعريف ، ووسائل التعريف البيولوجية التي تعتمد علي سمات معينة في شخص المستخدم متصلة ببنائه البيولوجي ، ومختلف أنواع المنتجات التي تزود كلمات سر آنية او وقتية متغيرة رقميا ، والمفاتيح المشفرة ، بل تضم هذه الطائفة ما يعرف بالأقفال الرقمية التي تحدد مناطق النفاذ .

- مجموعة الوسائل المتعلقة بالتحكم بالدخول والنفاذ الي الشبكة Access control وهي التي تساعد في التأكد من أن الشبكة ومصادرها قد استخدمت بطريقة مشروعة ، وتشمل من بين ما تشمل الوسائل التي تعتمد علي تحديد حقوق المستخدمين ، او قوائم أشخاص

1 راجع في ذلك : الباحث / حسين خلف موسي ، استراتيجية أمن المعلومات في ظل حروب الجيل السادس ، مرجع سابق ، ص22 وما بعدها

المستخدمين أنفسهم ، او تحديد المزايا الاستخدامية او غير ذلك من الإجراءات والأدوات والوسائل التي تتيح التحكم بمشروعية استخدام الشبكة ابتداءا .

- مجموعة الوسائل التي تهدف الي منع إفشاء المعلومات لغير المخولين بذلك وتهدف الي تحقيق سرية المعلومات **Data and message confidentiality** ، وتشمل هذه الوسائل من بين ما تشمل تقنيات تشفير المعطيات والملفات file and message encryption technology , وإجراءات حماية نسخ الحفظ الاحتياطية protection for backup copies on tapes, diskettes, etc. , والحماية المادية للأجهزة ومكونات الشبكات physical protection of physical LAN medium and devices واستخدام الفلترات والموجهات .

- مجموعة الوسائل الهادفة لحماية التكاملية (سلامة المحتوي) **Data and message integrity** وهي الوسائل المناط بها ضمان عدم تعديل محتوى المعطيات من قبل جهة غير مخولة بذلك ، وتشمل من بين ما تشمل تقنيات الترميز والتواقيع الرقمية وبرمجيات تحري الفيروسات وغيرها .

-مجموعة الوسائل المتعلقة بمنع الإنكار (إنكار التصرفات الصادرة عن الشخص) **Non-repudiation** ، وتهدف هذه الوسائل الي ضمان عدم قدرة شخص المستخدم من إنكار انه هو الذي قام بالتصرف ، وهي وسائل ذات أهمية بالغة في بيئة الأعمال الرقمية والتعاقدات علي الخط ، وترتكز هذه الوسائل في الوقت الحاضر علي تقنيات التوقيع الرقمي وشهادات التوثيق الصادرة عن طرف ثالث.

-وسائل مراقبة الاستخدام وتتبع سجلات النفاذ او الأداء (الاستخدام) Logging

and Monitoring ، وهي التقنيات التي تستخدم لمراقبة العاملين علي النظام لتحديد الشخص الذي قام بالعمل المعين في وقت معين ، وتشمل كافة أنواع البرمجيات والسجلات الرقمية التي تحدد الاستخدام.

2. وسائل الأمن الأكثر استخداما في بيئة نظم المعلومات¹

أ. برمجيات كشف ومقاومة الفيروسات:

بالرغم من أن تقنيات مضادات الفيروسات تعد الأكثر انتشارا وتعد من بين وسائل الأمن المعروفة للعموم ، إلا أنها حجم تطبيق هذه التقنيات واستراتيجيات وخطة التعامل معها تكشف عن ثغرات كبيرة وعن أخطاء في فهم دور هذه المضادات ، وبالعموم ثمة خمسة آليات أساسية لكيفية تحري هذه المضادات للفيروسات التي تصيب النظام ، كما ثمة قواعد أساسية تحقق فعالية هذه الوسائل والتي تعتمد في حقيقتها علي الموازنة ما بين ضرورات هذه التقنيات لحماية النظام وما قد يؤثره الاستخدام الخاطئ لها علي الأداء وفعالية النظام .

- الجدران النارية Firewall والشبكات الافتراضية الخاصة virtual private

networks : تطورت الجدران النارية بشكل متسارع منذ نشأتها حين كانت تقوم بتصفية حركة البيانات اعتمادا علي قوانين ومعاملات بسيطة . أما برمجيات الجدران النارية الحديثة ، ورغم أنها لا تزال تقوم باستخدام أسلوب فلتر وتصفية البيانات الواردة ، فإنها تقوم بعمل ما هو اكثر بكثير مثل إنشاء الشبكات الافتراضية الخاصة virtual private networks ، رقابة محتوى البيانات الوقاية من الفيروسات ، وحتى إدارة نوعية الخدمة quality of

1 راجع في ذلك : المحامي/ يونس عرب، أمن المعلومات ماهيتها وعناصرها واستراتيجياتها ، مرجع السابق ، ص28 وما بعدها .

service ، وهذه الخدمات جميعها تعتمد علي ميزة أساسية وهي أن الجدران النارية تقع علي طرف الشبكة ، وخلال العقد الماضي ، كانت الجدران النارية ببساطة ، مجرد أدوات بسيطة تعمل كمنفذ للإنترنت - او بكلمات أخرى كحراس علي طرف الشبكة - تقوم بتنظيم حركة البيانات وحفاظ علي أمن الشبكة . وقد ظهرت أول الجدران النارية للشبكات في عام 1980 وكانت عبارة عن موجهات تستخدم في تقسيم هذه الشبكات الي شبكات محلية LAN صغيرة . وكانت مثل هذه الجدران النارية توضع في مواقعها هذه للحد من انتشار المشاكل التي يواجهها جزء من الشبكة الي الأجزاء الأخرى . وقد تم استخدام أول الجدران النارية لتحقيق الأمن في أوائل التسعينات ، وكانت عبارة عن موجهات لبروتوكول IP مع قوانين فلترة كانت تبدوا كالتالي : اسمح لفلان بالدخول والنفاذ الي الملف التالي . او امنع فلان (او برنامجا) من الدخول من المنطقة (او المناطق) التالية . وقد كانت هذه الجدران النارية فعالة ، ولكنها محدودة . حيث كان من الصعب في العادة إتقان وضع قوانين فلترة البيانات ، ومن الصعب في بعض الأحيان تحديد أجزاء التطبيقات المراد منعها من النفاذ الي الشبكة . وفي أحيان أخرى كانت عناصر الشبكة ، مثل الموظفين العاملين ضمنها ، تتغير ، مما كان يستدعي تغيير القوانين ، ولذلك ، كان الجيل التالي من الجدران النارية اكثر قدرة واكثر مرونة للتعديل.

ومن هذه البدايات البسيطة ، دفع التنافس الحاد بين المزودين للحصول علي حصة سوقية من سوق الجدران النارية ، الي المزيد من الابتكارات ، ليس فقط في مجال تسريع أداء الجدران النارية وتقديم خدماتها ، بل وأيضا في تضمينها قدرات متعددة تفوق ما كان متوفرا في تلك الأيام ، وتمثل هذه القدرات بما يلي :-

-التحقق من هوية المستخدمين :- ذلك إن أول ما إضافة المطورون الي الجدران النارية الأولى كانت القدرات القوية للتحقق من الهوية ، وإذا كانت السياسات الأمنية التي تتبعها المؤسسة تسمح بالنفوذ الي الشبكة من شبكة خارجية ، مثل الإنترنت ، فانه لا بد من استخدام ميكانيكية ما للتحقق من هوية المستخدمين . والتحقق من الهوية يعني ببساطة التأكد من صحة هوية المستخدم بشكل يتجاوز مجرد التحقق من اسم المستخدم والكلمات السرية والتي لا تعتبر بحد ذاتها وسيلة قوية للتحقق من هوية المستخدمين .ذلك انه وعلي وصلة غير خاصة ، مثل وصلة غير مشفرة عبر الإنترنت ، فان أسماء المستخدمين وكلماتهم السرية يمكن نسخها وإعادة استخدامها Replay Attacks ، أما الأساليب القوية للتحقق من هوية المستخدمين فتستخدم أساليب التشفير مثل الشهادات الرقمية Certificates ، او برمجيات حساب الشفريات الرقمية الخاصة . وبواسطة الشهادات الرقمية يمكن تقادي هجمات إعادة الاستخدام حيث يتم نسخ اسم المستخدم وكلماته السرية وإعادة استخدامها للنفوذ الي الشبكة .

- الشبكات الافتراضية الخاصة :- أما الإضافة الثانية الي الجدران النارية للإنترنت فكانت التشفير البيني للجدران النارية firewall - to firewall وكان اول منتج من هذا النوع هو Ans interlock ، وهذه المنتجات هي ما ندعوها اليوم بالشبكات الافتراضية الخاصة virtual private networks . وهذه الشبكات خاصة لأنها تستخدم التشفير ، وهي افتراضية خاصة لأنها تستخدم الإنترنت وشبكات عامة لنقل المعلومات الخاصة . ورغم أن الشبكات الافتراضية الخاصة كانت متوفرة قبل برمجيات الجدران النارية باستخدام الموديمات او الموجهات للتشفير لكنها أصبحت تستخدم فيما بعد ضمن برمجيات الجدران النارية . ويمكن باستخدام تقنيات الشبكات الافتراضية الخاصة أن تقوم المؤسسات باستبدال مرافق الاتصالات المؤجرة وقنوات مشفرة عبر الشبكات العامة مثل الإنترنت .

-مراقبة المحتوى **Content Screening** :- وخلال العامين الماضيين اصبح من

الشائع استخدام الجدران النارية كأدوات لمراقبة المحتوى الوارد الي الشبكة .

-ومن بعض الإضافات التي وضعت في برمجيات الجدران النارية هي البحث عن

الفيروسات ، ومراقبة عناوين الإنترنت ، منع برمجيات جافا ، وبرمجيات فحص ومراقبة الكلمات السرية.

- **الجدران النارية الخاصة firewall appliances** :- وهو جيل جديد من الجدران

النارية الذي بدأ المزودون بطرحه خلال العام الماضي .وهذا الجيل يحتوي علي عدد من التقنيات بما في ذلك حلول جدران نارية جاهزة turnkey بمعنى أنها لا تحتاج الي إعداد من قبل المستخدم ويمكن البدء باستخدامها فور الحصول عليها دون الحاجة الي إجراء تعديلات خاصة علي نظام التشغيل او البنية التحتية المستخدمة.

لقد انتقلت وسائل حماية الإنترنت من مستويات الحماية الفردية او ذات الاتجاه الفردي ، التي تقوم علي وضع وسائل الحماية ومنها الجدران النارية في المنطقة التي تفصل الشبكة الخاصة عن الموجهات التي تنقل الاتصال الي الشبكة العالمية¹ (الإنترنت) ، الي مستويات الأمن المتعددة والتي تقوم علي فكرة توفير خطوط إضافية من الدفاع بالنسبة لنوع معين من المعلومات او نظم المعلومات داخل الشبكة الخاصة ، وتعتمد وسائل الأمن متعددة الاتجاهات والأغراض آليات مختلفة لتوفير الأمن الشامل للنظام COMPREHENSIVE SECURITY SYSTEM . وتتضمن ثلاثة مناطق أساسية :

1 راجع في ذلك : د/ جمال عبده عبد العزيز سيد ، الجهود الدولية لمكافحة الجرائم المعلوماتية في اطار أدلة إثباتها في التشريعات العربية ، مرجع سابق ، ص13 وما بعدها

الأولي : إدارة خطوات الأمن وتشمل الخطط والاستراتيجيات وأغراضها وكذلك المنتجات وقواعد الإنتاج و البحث والتحليل .

الثانية : أنواع الحماية وتشمل الوقاية او الحماية والتحقيق والتحري والتصرف .

الثالثة : وسائل الحماية وتشمل حماية النظم والخوادم وحماية البنية التحتية للشبكة .

ب. التشفير 1:

تحظى تقنيات وسياسات التشفير في الوقت الحاضر باهتمام عالي في ميدان أمن المعلومات ، ومرد ذلك أن حماية التشفير يمثل الوسيلة الأكثر أهمية لتحقيق وظائف الأمن الثلاثة ، السرية والتكاملية وتوفير المعلومات ، فالتشفير تقنيات تدخل في مختلف وسائل التقنية المنصبة علي تحقيق حماية هذه العناصر ، فضمان سرية المعلومات اصبح يعتمد من بين ما يعتمد علي تشفير وترميز الملفات والمعطيات بل تشفير وسائل التثبيت وكلمات السر ، كما أن وسيلة حماية سلامة المحتوي تقوم علي تشفير البيانات المتبادلة والتثبت لدي فك التشفير أن الرسالة الرقمية لم تتعرض لأي نوع من التعديل او التغيير ، ويعد التشفير بوجه عام وتطبيقاته العديدة وفي مقدمتها التواقيع الرقمية ، الوسيلة الوحيدة تقريبا لضمان عدم إنكار التصرفات عبر الشبكات الرقمية ، وبناء علي ذلك فان التشفير يمثل الاستراتيجية الشاملة لتحقيق أهداف الأمن من جهة ، وهو مكون رئيس لتقنيات ووسائل الأمن الأخرى ، خاصة في بيئة الأعمال الرقمية والتجارة الرقمية والرسائل الرقمية وعموما البيانات المتبادلة بالوسائط الرقمية .

1 راجع في ذلك : ا . د / عبد العزيز ملحم بربر ، امن الشبكات والإنترنت ، حلقة علمية بعنوان الإنترنت والإرهاب ، جامعة نايف العربية للعلوم الأمنية ، 15-19/11/2008 ، ص 7 .

ومن حيث مفهومه ، فإن التشفير يمر بمرحلتين رئيسيتين ، الأولى تشفير النص علي نحو يحوله الي رموز غير مفهومة او مقروءة بلغة مفهومة ، والثانية ، فك الترميز بإعادة النص المشفر الي وضعه السابق كنص مفهوم ومقروء ، وهذه المسألة تقوم بها برمجيات التشفير التي تختلف أنواعها ووظائفها . أما من حيث طرق التشفير ، فثمة التشفير الترميزي ، والتشفير المعتمد علي مفاتيح التشفير ، التي قد تكون مفاتيح عامة او خاصة او مزيجا منها ، وللوقوف علي ابرز أغراض وعناصر التشفير وطرقه التقنية نورد تاليا مواد مختارة تتناول هذه المسائل مع الإشارة الي مصادرها .

ثانيا : أغراض حماية البيانات الرئيسية¹ :

1 - السرية **CONFIDENTIALITY** : التأكد من ان المعلومات لا تكشف ولا

يطلع عليها من قبل أشخاص غير مخولين بذلك .

2 - التكاملية وسلامة المحتوي **INTEGRITY** : التأكد من أن محتوى المعلومات

صحيح لم يتم تعديله أو العبث به وبشكل خاص لن يتم تدمير المحتوي أو تغييره عن طريق تدخل غير مشروع .

3 - استمرارية توفر المعلومات أو الخدمة **AVAILABILITY** : التأكد من أن

مستخدم المعلومات لن يتعرض الي إنكار استخدامه لها أو دخوله إليها .

1 راجع في ذلك : المحامي/ يونس عرب، أمن المعلومات ماهيتها وعناصرها واستراتيجياتها ، مرجع السابق ،

ثالثا : مناطق أمن المعلومات¹

1 - أمن الاتصالات : ويراد بأمن الاتصالات حماية المعلومات خلال عملية تبادل

البيانات من نظام إلي آخر .

2 - أمن الأدوات او الوسيط الرقمي : ويراد به حماية المعلومات داخل النظام بكافة

أنواعها وأنماطها وداخل أي وسيط رقمي كحماية نظام التشغيل وحماية برامج التطبيقات وحماية برامج إدارة البيانات وحماية قواعد البيانات بأنواعها المختلفة ..

ولا يتحقق أمن المعلومات دون توفير الحماية المتكاملة لهذين القطاعين عبر معايير أمنية

تكفل توفير هذه الحماية ، ومن خلال مستويات أمن متعددة ومختلفة من حيث الطبيعة.

رابعا : أنماط ومستويات أمن المعلومات² :

1 - الحماية المادية : وتشمل كافة الوسائل التي تمنع الوصول إلي نظم المعلومات

وقواعدها كالأقفال والحواجز والغرف المحصنة وغيرها من وسائل الحماية المادية التي تمنع

الوصول إلي الأجهزة والوسائط الرقمية ذات الأهمية في عملية التقاضي الرقمي .

2- الحماية الشخصية : وهي تتعلق بالموظفين العاملين علي النظام التقني المعني من

حيث توفير وسائل التعريف الخاصة بكل منهم وتحقيق التدريب والتأهيل للمتعاملين لتحقيق

1 راجع في ذلك : الباحث / حسين خلف موسي ، استراتيجية أمن المعلومات في ظل حروب الجيل السادس ، مرجع سابق ، ص 27.

2 راجع في ذلك : المحامي/ يونس عرب، أمن المعلومات ماهيتها وعناصرها واستراتيجياتها ، مرجع السابق ، ص38 .

الاستفادة القصوى من التحول للرقمية إلى جانب الوعي بوسائل الأمن ومخاطر الاعتداء علي المعلومات.

3 - الحماية الإدارية : ويراد بها سيطرة جهة الإدارة علي النظم المعلوماتية وقواعدها وإدارة التكنولوجيا إدارة ذكية مثل التحكم بالبرمجيات الخارجية او الأجنبية داخل الهيئات والمؤسسات ، ومسائل التحقيق بإخلالات الأمن ، ومسائل الإشراف والمتابعة لأنشطة الرقابة.

4 - الحماية الإعلامية- المعرفية : كالسيطرة علي إعادة إنتاج المعلومات وعلي عملية إتلاف مصادر المعلومات الحساسة عند اتخاذ القرار بعدم استخدامها وحظر نشرها¹.

خامسا : الوقاية من مخاطر الاعتداء علي المعلومات ²

في ميدان حماية الاتصالات وحماية الوسائط الرقمية يعبر عن إجراءات الوقاية بخدمات الأمن ، ولا يقصد بها الخدمات بالمعني المعروف ، وإنما أطلق هذا التعبير جراء نشوء شركات متخصصة بأمن المعلومات تقدم هذه الخدمات ، وبالعوموم فان هناك خمسة أنواع أساسية لخدمات الأمن تستهدف حماية خمسة عناصر رئيسة في ميدان المعلومات وهي:

1 - خدمات (وسائل) حماية التعريف Identification And Authentication

هذه الخدمات تهدف إلي التثبت من الهوية وتحديدًا عندما يقوم شخص ما بالتعريف عن نفسه فان هذه الخدمات تهدف إلي التثبت من إنه هو الشخص نفسه ولهذا فان التعريف يعد الوسائل

1 راجع في ذلك : القاضي د/ أسامة أحمد عبد النعيم ، " الضوابط القانونية لقرار حظر النشر ، الضوابط

القانونية لقرار حظر النشر " ، بمؤتمر القانون والإعلام ابريل 2017 ، ص 8 وما بعدها .

2 راجع في ذلك : د/ يونس عرب - امن المعلومات ماهيتها و عناصرها و إستراتيجيتها، مرجع سابق ، ص 37

وما بعدها .

التي تحمي من أنشطة التخفي والتتكر ومن هنا فإن هناك نوعين من خدمات التعريف الأول تعريف الشخصية وأشهر وسائلها كلمات السر وثانيها التعريف بأصل المعلومات كالتثبت من أصل الرسالة .

2 - خدمات (وسائل) السيطرة علي الدخول Access Control : وهذه الخدمات

تستخدم للحماية ضد الدخول غير المشروع إلي مصادر الأنظمة والاتصالات والمعلومات ويشمل مفهوم الدخول غير المصرح به لأغراض خدمات الأمن الاستخدام غير المصرح به والإفشاء غير المصرح به ، والتعديل غير المصرح به ، الإلتاف غير المصرح به ، وإصدار المعلومات والأوامر غير المصرح بها ولهذا فإن خدمات التحكم بالدخول تعد الوسائل الأولية لتحقيق الدخول والتثبت منه ¹.

3 - خدمات (وسائل) السرية Data And Message Confidentiality : هذه

الخدمات تحمي المعلومات من الإفشاء للجهات غير المصرح لها بالحصول عليها ، والسرية تعني بشكل عام إخفاء المعلومات من خلال تشفيرها علي سبيل المثال او من خلال وسائل أخرى كمنع التعرف علي حجمها او مقدارها او الجهة المرسله إليها.

4 - خدمات (وسائل) حماية التكاملية وسلامة المحتوي Data and message Integrity

هذه الخدمات تهدف إلي الحماية من مخاطر تغيير البيانات خلال عمليات إدخالها او معالجتها او نقلها وعملية التغيير تعني بمفهوم الأمن هنا الإلغاء او التحوير او إعادة تسجيل

1 راجع في ذلك : (تاريخ آخر دخول : 2021/1/13)

- <https://www.frontlinedefenders.org/ar/programme/digital-protection>
- https://www.isaca.org/credentialing/crisc?cid=sem_2002368&Appeal=sem&gclid=Cj0KCQiA0fr_BRDaARIsAABw4EumO0AObSaP472q11TtdPV52Hskrsfb10mSEcChmlh-4SUQtK3I9TgaAhxIEALw_wcB
- <https://etc.ksu.edu.sa/ar/pages/report/main/security-risk>

جزء منها او غير ذلك وتهدف هذه الوسائل أيضا إلى الحماية من أنشطة تدمير المعطيات بشكل كامل او إلغائها دون إذن¹ .

5 - خدمات (وسائل) منع الإنكار Non-repudiation: وهذه الخدمات تهدف إلى

منع الجهة التي قامت بالتصرف من إنكار حصول نقل البيانات او النشاط من قبلها .

وتعد الخدمات الخمس المتقدمة مناطق الحماية الأساسية في مجال المعلومات ، فالحماية يتعين أن تمتد إلى التعريف ، أنشطة الدخول ، السرية ، سلامة المحتوي ، منع عدم الإنكار ولا بد أن يصاحب كل ذلك تدخل تشريعي² .

سادسا : إستراتيجية أمن الإنترنت³

تتصب أساسي أمن المعلومات في حقل تحقيق أمن الإنترنت علي مواضع ثلاث :-
أمن الشبكة ، أمن التطبيقات ، أمن النظم . وكل منها ينطوي علي قواعد ومتطلبات تختلف عن الأخرى ويتعين أن تكون أنظمة الأمن في هذه المواضع الثلاث متكاملة مع بعضها حتي تحقق الوقاية المطلوبة لأنها بالعموم تنطوي أيضا علي اتصال وارتباط بمستويات الأمن العامة كالحماية المادية والحماية الشخصية والحماية الإدارية والحماية الإعلانية . وفيما تقدم اشرنا الي

1 راجع في ذلك : الباحث / حسين خلف موسي ، استراتيجية أمن المعلومات في ظل حروب الجيل السادس ، مرجع سابق ، ص 30.

2 جرم المشرع بالمادة (36- 48) من قانون رقم 101 لسنة 2020 بإصدار قانون حماية البيانات الشخصية ، الجرائم التي تصدر من المتحكم والمعالج والحائز للبيانات .

3 راجع في ذلك : الباحث / حسين خلف موسي ، استراتيجية أمن المعلومات في ظل حروب الجيل السادس ، مرجع سابق ، ص 31 وما بعدها .

العناصر المتصلة بأمن النظم والبرمجيات والمعطيات وبقي أن نشير في هذا المقام الي أمن الشبكات :-

إن ما يحمي من خلال أمن الشبكة هو عملية الاتصال والتبادل بين أحد كمبيوترات الشبكة (النظام النهائي سواء أكان نظام الزبون أن نظام المستضيف (الخادم) وبين كمبيوتر آخر ضمن الشبكة ، فإذا ارتبط النظام النهائي بالإنترنت مباشرة دون وجود وسائل أمن ما بين هذا النظام والشبكة فان أية حزمة بيانات مرسله قد يلحق بها ما يلي :

أ - قد يتم تغييرها خلال عملية النقل

ب - قد لا تظهر من حيث مصدرها من الجهة التي قدمت منها

ج - قد تكون جزء من هجوم يستهدف النظام

د - قد لا تصل الي العنوان المرسله اليه

هـ - قد يتم قراءتها والاطلاع عليها وإفشاؤها من الغير .

ويهدف أمن الشبكات من جهة أخرى الي حماية الشبكة نفسها وإظهار الثقة لدي مستخدم النظام النهائي بتوفر وسائل الحماية في تعامله مع الشبكة وكذلك إظهار الشبكة ذاتها بانها تحتوي علي وسائل أمن لا تتطلب معها أن يكون كمبيوتر المستخدم محتويا علي وسائل خاصة.

وتتضمن وسائل أمن الشبكة ما يلي :-

1 - التعريف والسلامة من خلال تزويد نظام المستقبل بالثقة في حماية حزم المعلومات

والتأكد من أن المعلومات التي وصلت لم يتم تعديلها .

2 - السرية : حماية محتوى حزم المعلومات من الإفشاء إلا للجهات المرسله إليها .

3 - التحكم بالدخول : تقييد الاتصالات بحصرها ما بين النظام المرسل والنظام المستقبل.

سابعا : إطار بناء خطط واستراتيجيات الأمن¹

هناك العديد من قوائم التدقيق والمراجعة حول مسائل أمن المعلومات ومتطلبات سياسات واستراتيجيات أمن المعلومات والنظم والاتصالات ، وتقوم بالأساس علي توفير نوع من دليل المراجعة الذي يساعد المؤسسات او الأفراد في بناء أساسي الأمن وتحديد اطار عام لواجبات الموظفين والمستشارين و المعنيين بشؤون إدارة نظم المعلومات والاتصال وتطبيقاتهما وبنفس الوقت تقدم هذه القوائم او أدلة المراجعة المؤسسات والأفراد اطار عاما لفهم عناصر ومتطلبات بناء نظم الأمن الخاصة بالكمبيوتر والشبكات.

ومن بين المسائل التي تعالجها عادة هذه القوائم :-

-مسائل واجبات جهات الإدارة للتحقق من وجود سياسة أمن المعلومات موثقة ومكتوبة والتحقق من وجود عمليات تحليل المخاطر وخطة الأمن وبناء الأمن التقني وسياسة إدارة الاتصالات الخارجية ، ومدى معرفة واطلاع الموظفين علي السياسة الأمنية ومعرفتهم بواجباتهم ، ومدى توفر تدريب علي مسائل الأمن وما اذا كان يخضع الموظفون الجدد لتدريب وتعريف حول محتوى الخطة .

1 راجع في ذلك : المحامي/ يونس عرب، أمن المعلومات ماهيتها وعناصرها واستراتيجياتها ، مرجع السابق ،

ص39 وما بعدها .

-مسائل تنظيم شؤون إدارة الأمن ، والتي تتعلق بوجود جهة مختصة بذلك في المؤسسة وما اذا كان هنالك دليل مكتوب ، وخطط ومسؤولية التعامل مع إجراءات التنفيذ والتعريف والتعامل مع الحوادث ومع خطط الطوارئ وغيرها.

-مسائل الموظفين أنفسهم من حيث مدى فحص التأهيل والكفاءة ومدى التزام الموظفين بتحقيق معايير الأمن علي المستوى الشخصي او فيما يتعلق بواجباتهم ، وأغراضها المتصلة بالأمن لدي تعيين الموظفين وخلال عملهم ولدي انتهاء خدمتهم لأي سبب ، وتتصل أيضا بمدى توفر نصوص عقدية خاصة في عقود الموظفين ومدى توفر وصف دقيق بواجباتهم الوظيفية المتصلة بالحقاق المعلومات .

-مسائل جهات تزويد الخدمة او المشورة كالمستشارين والمدققين وغيرهم من حيث تغطية عقود التعامل معهم لمسائل الأمن المختلفة .

-مسائل تصنيف المعلومات من حيث توفرها ومعاييرها .

-مسائل البرمجيات من حيث سياسات شرائها واستخدامها وتنزيلها ومسائل الرخص المتصلة بها وآليات التعامل مع البرمجيات المطورة داخليا وحقوق الوصول إليها واستخدامها ، ومسائل حماية البرمجيات التقنية والقانونية .

-مسائل الأجهزة والمعدات من حيث توفر تصور للاحتياجات وتوفير المتطلبات ومعايير توظيف الأجهزة في العمل ، واستخداماتها وإلغاء استخدامها ومسائل صيانتها والتدقيق لها.

-مسائل التوثيق ، وهي التي تتعلق بمدى توفر استراتيجية التوثيق لكافة عناصر النظام ولكافة مرتكزات وعمليات خطط الأمن وسياساتها.

-المسائل المتصلة بوسائط التخزين خارج النظام من حيث تحديد وسائط التخزين المستخدمة وتبويبها وحفظها والوصول إليها وتبادلها وإتلافها .

-مسائل التعريف والتوثيق من شخصية المستخدم وحدود الصلاحيات والتفويض ، وتتعلق بالتحقق من توفر سياسة التحكم بهذه العناصر والوسائل المستخدمة في تحديد الهوية والتوثيق من المستخدم ، واستراتيجيات حماية وسائل التعريف تقنيا وإداريا، ومدى صلاحية المستخدمين من الخارج او من داخل المؤسسة بشأن الوصول للمعلومات او قطاعات منها ، ومسائل التحقق من تصرفات المستخدم ، مسائل أمن النظام من حيث توفر وسائل التثبيت من حيث وقت الاستخدام و المستخدمين .

-مسائل الاتصالات من حيث السيطرة علي وسائل وتطبيقات الاتصالات الداخلية والخارجية وتوثيق حركات الاتصال وحماية عمليات الاتصال والمعايير التقنية المستخدمة في ذلك واستراتيجيات سرية ورقابة وتتبع واستخدام البريد الرقمي .

-مسائل إدارة الملفات وسجلات الأداء واستخدام النظام من حيث توفر وسائل توثيقها وأرشفتها والتثبيت من جهات الأنشاء والتعديل والتعامل مع الملفات وقواعد البيانات والبرامج التطبيقية .

-مسائل النسخ الاحتياطية من البيانات من حيث وقت عمل النسخ الاحتياطية وتخزينها واستخداماتها وتبويبها وتوثيقها وتشفيرها اذا كانت مما يتطلب ذلك .

-مسائل الحماية المادية من حيث التوثيق من توفير وسائل وإجراءات الحماية للأجهزة الكمبيوتر والشبكات والبنى التحتية من ومسائل الطاقة والتوصيلات ومدى توفر وسائل الوقاية

من الحوادث الطبيعية او المتعمدة إضافة الي وسائل حماية مكان وجود الأجهزة والوسائط وأدلة الأمن المكتوبة ، والوسائل المادية للوصول الي الأجهزة واستخدامها من المخولين بذلك .

-مسائل التعامل مع الحوادث والاعتداءات ، من حيث توفر فريق لذلك وأغراضها التي يقوم بها الفريق لهذه الغاية إضافة الي وجود ارتباط مع جهات التحقيق الرسمية وجهات تطبيق القانون وجهات الخبرة المتخصصة بالمسائل المعقدة او التي لا تتوفر كفاءات للتعامل معها داخل المؤسسة .

-مسائل خطط الطوارئ وخطط التعافي لتخفيف الأضرار والعودة للوضع الطبيعي .

-مسائل الأعلام المتعلقة بالمعلومات المتعين وصولها للكافة او لقطاعات محددة والتحقق من وضوح استراتيجية التعامل الإعلامي مع الحوادث والاعتداءات المتحققة .

ومع إن قوائم المراجعة هذه تتباين من مؤسسة الي أخرى ، ومن شخص الي آخر ، تبعاً للواقع والاحتياجات وطبيعة النظام والمعلومات والتطبيقات العملية إلا أن الكثير منها يصلح كإطار عام ومرجعية لدي وضع هذه القوائم والأدلة .

الفرع الثالث

الحماية القانونية لأمن المعلومات

ويقصد بالحماية القانونية تجريم أية صورة من صور التعدي علي البيانات الخاصة بعملية

التقاضي الرقمي بكافة مراحلها ، والتي من صورها¹ :

- التزوير المعلوماتي؛ ويقصد به تغيير حقيقة المحررات أو الوثائق الرقمية.

- الدخول إلي النظام المعلوماتي للمحكمة من قبل الأشخاص غير المرخص لهم ومحاولة

حصولهم علي معلومات من هذا النظام.

- تدمير المعلومات وإتلافها علي نحو يعدم الاستفاداة منها، والتلاعب في بيانات شبكة

المحكمة .

- إتلاف الأدلة الرقمية

- التسبب في إحداث أزمات رقمية

ونشير هنا إلي قصور النصوص القانونية في التشريعات العربية الخاصة بالتقاضي الرقمي

والتقاضي عن بعد وكذلك التقاضي الذاتي الحالية وتطبيقاته في البلدان العربية قاطبة ولعل السبب

في ذلك تأخر التحول الي الرقمية ببعض البلدان او بطئ التحول ببعض الآخر بسبب نقص

الإمكانيات المادية وما يعانیه الاقتصاد العالمي من تدهور خاصة بعد المرور بالعديد من الأزمات

1 راجع في ذلك : أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، الحماية الجنائية للحاسب

الآلي دراسة مقارنة ،دار النهضة العربية، الطبعة الأولى، مصر، سنة 2000 ، ص 3

والثورات والأوبئة والأمراض والتي من أشهرها فيروس كوفيد - 19 ، وهو ما يجعل مهمة القاضي العربي صعبة ويثقل كاهل الفقه الجنائي العربي في عملية تأصيل هذه الوقائع وتفسيرها، الأمر الذي يؤدي إلي صعوبة التكييف القانوني والوصول بالتقاضي الرقمي الي ارقى مستوياته كما حدث بالفعل بالعديد من دول العالم والتي سبقت في هذا المجال وعلي العكس من ذلك فإن الدول الأوروبية والولايات المتحدة الأمريكية وغيرها من الدول المتقدمة لديها تشريعات معلوماتية متقدمة، تستطيع من خلالها الحكم علي الأفعال المجرمة التي تقع عن طريق الحاسب الآلي والأنترنيت في مجال التقاضي الرقمي وهو وما سنعرض له بالمبحث التالي .

المطلب الرابع

موقف النظم القضائية المقارنة

في ظل التطور التكنولوجي بات ارتكاب الجرائم من دولة لأخرى من السهولة بمكان ، وتعرف الجريمة في ذلك بالجريمة المنظمة نتيجة مزاوله الأنشطة الإجرامية عبر حدود الدول. ولذلك قامت الدول حرصاً منها علي احترام الخصوصية للأشخاص ومواجهة الجرائم بإبرام العديد من الاتفاقيات الدولية¹ لمكافحة هذه الظاهرة هذا بجانب الضمانات التي أقرتها الاتفاقيات والمواثيق الدولية .

1 راجع في ذلك : الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المصادق عليها بموجب المرسوم الرئاسي رقم 252/14 المؤرخ في 8 سبتمبر 2014 علي جريدة رسمية عدد 57 , و راجع أيضا : اتفاقية بودابست للإجرام المعلوماتي لسنة 2001 .

الفرع الأول

موقف التشريعات الغربية

تنبهت الدول الغربية وخصوصا أوروبا في وقت مبكر (بالمقارنة مع غيرها) لمخاطر الجريمة وصورها ، ولعل ذلك سببه دخول الحاسب وتطبيقاته في وقت مبكر في مختلف مجالات الحياة ، ومختلف القطاعات حكومية وغير حكومية ، الأمر الذي جعل المجتمع الدولي يفتن إلي ضرورة مواجهتها بتشريعات عقابيه خاصة ، فعقدت الاتفاقية الأوربية لمكافحة الإجرام المعلوماتي والمسماة " بودابست عام 2001" لذلك كان لهذه الدول السبق في استصدار التشريعات المتعلقة بمكافحة الجريمة المعلوماتية.

فعلي سبيل المثال نجد المشرع الفرنسي حمي المجتمع من هذه الظاهرة الإجرامية الخطيرة بفرض قواعد قانونيه تتدخل لمكافحة الإجرام المعلوماتي بالإضافة الي ما يمكن الاستعانة به من بعض القواعد القانونية القائمة في قانون العقوبات وبذلك يكون قانون العقوبات الفرنسي قد تصدى للجرائم المعلوماتية من خلال تطبيق القواعد القانونية القائمة علي الجرائم الرقمية وكذلك فرض قواعد قانونيه جديده لمواجهة الجرائم المعلوماتية ولم يكن هناك خلاف في الفقه والقضاء الفرنسي علي إمكانية تطبيق القواعد القانونية بقانون العقوبات الفرنسي علي الجرائم المعلوماتية المتعلقة بالمكونات المادية للأنظمة المعلوماتية مثل السرقة والإتلاف والنصب وخيانة الأمانة ... الخ ، لذلك اهتمت فرنسا بتطوير قوانينها الجنائية للتوافق مع المستجدات الإجرامية : حيث أصدرت في عام 1988 القانون رقم 19 / 88 الذي أضاف الي قانون العقوبات الجنائي جرائم الحاسب الآلي

والعقوبات المقررة له ، وقد قام المشرع الفرنسي بتعديل هذا القانون في عام 1994 رغبة منه في الحد من هذه الظاهرة الإجرامية¹ .

في حين أن المشرع الإنجليزي قد تأخر نسبيا في معالجة ظاهرة الجرائم المعلوماتية ، ومرد ذلك بصفه أساسية الي أن النظام الإنجليزي يعتمد علي السوابق القضائية ، إلي أن صدر أخيرا قانون إساءة استخدام الكمبيوتر في المملكة المتحدة عام 1990 ، حيث جرت في المملكة المتحدة تحقيقات أولية علي يد لجنة تدعي لجنة القانون الاسكتلندي ضمنها مذكرة استشارية معللة نشرت في عام 1982 ، ثم قدمت تلك اللجنة تقريرا تم نشره عن جرائم الكمبيوتر ، ومن ثم قامت لجنة أخرى تدعي بعد ذلك بتقديم تقرير عن الدراسات التي تمت والتي بدأت من عام 1981 حتي عام 1990 وجاء في تقرير هذه اللجنة أن هناك ثلاثة وسبعون محاولة غش معلوماتي حققت خسائر قدرها 1 ، 1 مليون جنية إسترليني خلال الفترة من عام 1987 الي عام 1990 وقد تابعت لجنة القانون التقديرات النهائية عام 1989 وتبع ذلك الموافقة علي إصدار قانون إساءة استخدام الكمبيوتر أصدر في يوليو عام 1990 ودخل حيز التنفيذ في أغسطس عام 1990 م .

وكذلك **الولايات المتحدة الأمريكية** شرعت قانونا خاصا بحماية أنظمة الحاسب الآلي 1976م_ 1985م ، وفي عام 1985 حدد معهد العدالة القومي خمسة أنواع رئيسة للجرائم المعلوماتية وهي جرائم الحاسب الآلي الداخلية ، جرائم الاستخدام غير المشروع عن بعد ، جرائم التلاعب بالحاسب الآلي ، دعم التعاملات الإجرامية ، وسرقة البرامج الجاهزة والمكونات المادية للحاسب . وفي عام 1986 صدر قانون تشريعي يحمل الرقم 1213 عرف فيه

1 راجع في ذلك : المستشار/ ايمن رسلان ، جرائم المعلوماتية والإنترنت " بين الواقع الافتراضي والواقع بالتطبيق

علي مصر والوطن العربي ، "لسنة 2012 ، ص 157.

جميع المصطلحات الضرورية لتطبيق القانون علي الجرائم المعلوماتية ، كما وضعت المتطلبات الدستورية اللازمة لتطبيقه وعلي أثر ذلك قامت الولايات الداخلية بإصدار تشريعات خاصة بها للتعامل مع هذه الجرائم ، ومن ذلك قانون ولاية تكساس لجرائم الحاسب الآلي¹ .

1 وغير ذلك من الدول الأوروبية كالسويد وبريطانيا وكندا وهولندا والمجر وبولندا كل هذه الدول عدلت القوانين الجنائية ليتم إدخال الجرائم المعلوماتية في اطار قانوني ويتم تجريم كل ما يشملها من عمليات احتيال ونصب وملكية فكرية وإختراق أجهزة الآخرين وما الي ذلك انظر في ذلك : المستشار/ ايمن رسلان ، جرائم المعلوماتية والإنترنت " بين الواقع الافتراضي والواقع بالتطبيق علي مصر والوطن العربي ، "سنة 2012 ، ص156 . انظر أيضا

— Kristin Finklea : Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement ، January 15، 2015 ،

الفرع الثاني

موقف التشريعات العربية

عرفت الدول العربية مؤخرا مخاطر الجريمة المعلوماتية وتنبهت لها مما حدا ببعض المشرعين العرب إلى محاولة التصدي لهذا النوع المستحدث من الإجرام والذي فرضه الاستيراد النشط لتقنيات المعلومات وإدخالها في مختلف جوانب الحياة السياسية والاقتصادية والاجتماعية سواء علي صعيد الحكومات ، والتي بدأت تتبني المفاهيم التقنية وتطبيقاتها في العمل الإداري الحكومي وهو ما يسمى (بالحكومة الرقمية) وكذلك علي صعيد القطاع الخاص ، وحتى الأفراد حيث شهدت البلاد العربية مؤخرا إقبالا كبيرا علي استخدام الحاسب وتطبيقاته البرمجية ، وإن كان بشكل متفاوت من دولة الي أخرى .خصوصا بعد إبرام الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في 2010 والتي انضمت إليها مصر مؤخرا . ومن ثم أصبحت ملتزمة بموجب المادة الخامسة منها بتجريم بعض الأفعال المرتبطة بجرائم تقنيه المعلومات .

ف نجد إن المشرع الإماراتي قد عالج مسألة الجريمة المعلوماتية في القانون رقم 2 لعام 2006 ، وتعد تجربة المشرع الإماراتي تجربة رائدة في هذا المجال سواء فيما يتعلق بالنواحي الموضوعية او الإجرامية ، فتعد من أفضل التجارب العربية وأكثرها تقدما في مجال التصدي للجريمة المعلوماتية لما يتمتع به التشريع الإماراتي من سعة ومرونة في نطاق التجريم مما يتبع تغطية اكبر نسبة ممكنة من الاعتداءات الواقعة في المجال المعلوماتي والوقف علي تطورات البيئة الرقمية.

في حين أن المملكة العربية السعودية قد سبقت نظيراتها من الدول العربية في إصدار قانون جديد لمكافحة الجرائم المعلوماتية التي تشمل التهديد والابتزاز والتشهير بالآخرين في مواقع الإنترنت وإنشاء مواقع الإنترنت الإرهابية ، وأعلنت السلطات المختصة إنها ستقرض عقوبات

بالحبس لمدة عام واحد وغرامات لا تزيد علي 500 الف ريال فيما يعادل 133 الف دولار لجرائم القرصنة المرتبطة بالإنترنت وإساءة استخدام كاميرات الهواتف المحمولة كالتقاط صور دون تصريح إلا أن المملكة وفي رغبة من أجل تقنين هذا الوضع أصدرت تشريعا وطنيا في هذا الخصوص مؤخرا تحت مسمى " نظام مكافحة جرائم المعلوماتية السعودي"¹.

كما أن المشرع العماني كان له قصب السبق في هذا المضمار ، حيث نص علي تجريم كثير من صور الجرائم المعلوماتية وأصدرت السلطنة العمانية المرسوم السلطاني رقم 72 لسنة 2001 الذي يتضمن جرائم الحاسب الآلي وحدد فيه الالتقاط غير المشروع للمعلومات او البيانات ، وجرائم الدخول غير المشروع علي أنظمة الحاسب الآلي ، وجرائم التجسس والتصنت علي البيانات والمعلومات ، وانتهاك خصوصيات الغير او التعدي علي حقهم في الاحتفاظ بأسرارهم وتزوير البيانات او وثائق مترجمة أيا كان شكلها وإتلاف ومحو البيانات والمعلومات ، وأخيرا جرائم نشر واستخدام برامج الحاسب الآلي بما يشكل انتهاكا لقوانين حقوق الملكية والأسرار التجارية².

وعلي الجانب الآخر نجد أن هناك تشريعات لا توجد بها قوانين خاصه بالجرائم المعلوماتية وإن وجد نص قريب من الفعل المرتكب فإن العقوبة المنصوص عليها لا تتلاءم وحجم الأضرار المترتبة علي جريمة الإنترنت ، كما هو في مملكة البحرين، وكذلك لا يوجد تشريع خاص بالدولة الفلسطينية يتعلق بجرائم الكمبيوتر والإنترنت إلا انه يمكن ملاحظة هذه الجرائم عن طريق

1 راجع في ذلك : المستشار/ ايمن رسلان ، جرائم المعلوماتية والإنترنت ، مرجع سابق ، ص112

2 راجع في ذلك : د/ محمود صالح العادلي ، الفراغ التشريعي في مجال مكافحة الجرائم الإلكترونية ، ورقة عمل ص 20 ، وراجع كذلك المشرع الأردني ونصه علي قوانين تجابه الجرائم المعلوماتية .

تطويع نصوص قانون العقوبات الفلسطيني وكذا المشرع السوري لم يعالج الجريمة المعلوماتية كما يجب أن يكون .

اما بالنسبة للوضع في مصر فلقد جاءت معالجة الأمر من خلال معالجات جزئية مبدئياً وهو ما يدل علي اعتناء المشرع المصري بتجريم الجرائم المعلوماتية، ومن أهم تلك التشريعات ما يلي:

1- القانون رقم 143 لسنة 1994 بشأن الأحوال المدنية:

وتناول فيه المشرع المصري السجلات والدفاتر الرقمية، وعاقب علي تجريم الأفعال الماسة بها، واعتبر التزوير الحاصل فيها بمثابة التزوير الحادث في المحررات الرسمية المنصوص عليه في قانون العقوبات.

2- قانون رقم 82 لسنة 2002 لحماية حقوق الملكية الفكرية:

(وتتمتع بحماية هذا القانون برامج الحاسب الآلي وحقوق المؤلفين علي مصنفاتهم الأدبية والفنية وبرامج الحاسب الآلي) .

3- قانون رقم 15 لسنة 2004 بشأن تنظيم التوقيع الرقمي وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات.

وعلي الرغم من كون هذا القانون لم يقدم معالجة شاملة للمعاملات الرقمية لكنه يعد أول تشريع مصري يتعلق مباشرة بتنظيم المعاملات الرقمية، حيث أضفي هذا القانون المشروعية علي استخدام الوسائط الرقمية في تحرير وتبادل وحفظ المعلومات والمستندات إسهاماً منه في إضفاء الموثوقية علي تلك المعاملات، ومنح حجية قانونية للكتابة الرقمية وللتوقيع الرقمي في الإثبات.

1- **صدر مؤخراً بناءاً علي مناداة فقهاء القانون والقضاء قانون مكافحة قانون جرائم**

تقنية المعلومات رقم 175 لسنة 2018 والمكون من 45 مادة تناول فيها المشرع

ما يلي :

وضع تعريف البيانات والمعلومات الرقمية : (إنها كل ما يمكن إنشاؤه أو تخزينه ، أو معالجته ، أو تخليقه ، أو نقله ، أو مشاركته ، أو نسخه بواسطة تقنية المعلومات ؛ كالأرقام والأكواد والشفارات والحروف والرموز والإشارات والصور والأصوات وما في حكمها) م 1 ، **كما عرف البيانات شخصية إنها :** (أي بيانات متعلقة بشخص طبيعي محدد أو يمكن تحديده، بشكل مباشر أو غير مباشر عن طريق الربط بينها وبين بيانات أخرى) ، **والبيانات حكومية :** (بيانات متعلقة بالدولة أو أحد سلطاتها ، وأجهزتها أو وحداتها ، أو الهيئات العامة ، أو الهيئات المستقلة والأجهزة الرقابية ، وغيرها من الأشخاص الاعتبارية العامة وما في حكمها ، والمتاحة علي الشبكة المعلوماتية أو علي أي نظام معلوماتي أو علي حاسب أو ما في حكمها) ، و **المعالجة الرقمية :** (أي عملية رقمية أو تقنية تتم ؛ كلياً أو جزئياً ، لكتابة ، أو تجميع ، أو تسجيل ، أو حفظ ، أو تخزين ، أو دمج ، أو عرض ، أو إرسال ، واستقبال ، أو تداول ، أو نشر ، أو محو ، أو تسيير ، أو تعديل ، أو استرجاع ، أو استبدال للبيانات والمعلومات الرقمية، وذلك باستخدام أي وسيط من الوسائط أو الحاسبات أو الأجهزة الأخرى الرقمية أو المغناطيسية أو الضوئية أو ما يستحدث من تقنيات أو وسائط أخرى) ، و **تقنية المعلومات :** (أي وسيلة أو مجموعة وسائل مت اربطة أو غير مترابطة - تستخدم لتخزين ، واسترجاع ، وترتيب ، وتنظيم ، ومعالجة ، وتطوير ، وتبادل المعلومات أو البيانات ، ويشمل ذلك كل ما يرتبن بالوسيلة أو الوسائل المستخدمة سلكياً أو لاسلكياً) .

و **مقدم الخدمة** : (أي شخص طبيعي أو اعتباري يزود المستخدمين بخدمات تقنيات المعلومات والاتصالات، ويشمل ذلك من يقوم بمعالجة أو تخزين المعلومات بذاته أو من ينوب عنه في أي من تلك الخدمات أو تقنية المعلومات) .

و **المستخدم** : (كل شخص طبيعي أو اعتباري ، يستعمل خدمات تقنية المعلومات أو يستفيد منها بأي صورة كانت) ، و **النظام المعلوماتي** : (مجموعة برامج وأدوات معدة لغرض إدارة ومعالج- البيانات والمعلومات ، أو تقديم خدمة معلوماتية) ، و **شبكة معلوماتية** : (مجموعة من الأجهزة أو نظم المعلومات مرتبطة معاً ، ويمكنها تبادل المعلومات والاتصالات فيما بينها ، ومنها الشبكات الخاصة والعامة وشبكات المعلومات الدولية ؛ والتطبيقات المستخدمة عليها) ، و **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) . و **الاعتراض** : (مشاهدة البيانات أو المعلومات أو الحصول عليها بغرض التتصت أو التعطيل، أو التخزين أو النسخ، أو التسجيل ، أو تغيير المحتوى ، أو إساءة الاستخدام أو تعديل المسار أو إعادة التوجيه وذلك لأسباب غير مشروعة ودون وجه حق) ، و **الاختراق** : (الدخول غير المرخص به ، أو المخالف لأحكام الترخيص ، أو الدخول بأي طريقة غير مشروعة ، إلي نظام معلوماتي أو حاسب إلي أو شبكة معلوماتية، وما في حكمها) ، و **المحتوي** : (أي بيانات تؤدي بذاتها، أو مجتمعه مع بيانات أو معلومات أخرى إلي تكوين معلومة أو تحديد توجه أو اتجاه أو تصور أو معني أو الإشارة إلي بيانات أخرى) ، و **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) . (وهو ما يعدد اعتراف بالدليل الرقمي من جانب المشرع) ، و **حركة الاتصال** (بيانات المرور): (بيانات ينتجها نظام

معلوماتي تبين مصدر الاتصال ، وجهته والوجهة المرسل منها وإليها ، والطريق الذي سلكه ، وساعته وتاريخه وحجمه ومدته ، ونوع الخدمة) ، **والدعامة رقمية:** (أي وسيط مادي لحفظ وتداول البيانات والمعلومات الرقمية ومنها الأقراص المدمجة أو الأقراص الضوئية أو الذاكرة الرقمية أو ما في حكمها) . كما نص بالمادة (2) علي التزامات وواجبات مقدم الخدمة ، كما عالج المشرع الاعتداء علي سلامة شبكات وأنظمة وتقنيات المعلومات . وجرم بالمادة 13 : جريمة الانتفاع بدون وجه حق بخدمات الاتصالات والمعلومات وتقنياتها حيث نص علي :

(يعاقب بالحبس مدة لا تقل عن 3 شهور وبغرامة لا تقل عن 10 ألف جنيه ولا تجاوز 50 ألف جنيه أو بأحد هاتين العقوبتين، كل من انتفع بدون وجه حق عن طريق شبكة النظام المعلوماتي، أو إحدى وسائل تقنية المعلومات، بخدمة من خدمات اتصالات أو خدمات قنوات البث المسموع والمرئي) ، **وجرم بالمادة 14 :** (جريمة تجاوز حدود الحق في الدخول) ، **وبالمادة 15 :** جرم الدخول غير المشروع وعاقب بالمادة 16 : علي جريمة الاعتراض غير المشروع¹ كما عاقب بالمادة 17 : علي جريمة الاعتداء علي سلامة البيانات والمعلومات والنظم المعلوماتية² ، بالمادة 18 : عاقب علي جريمة الاعتداء علي البريد الرقمي أو المواقع أو الحسابات الخاصة³ ، وعاقب بالمادة 20 علي جريمة الاعتداء علي الأنظمة المعلوماتية

1) يعاقب بالحبس مدة لا تقل عن سنة وبغرامة لا تقل عن 50 ألف جنيه ولا تجاوز 250 ألف جنيه، أو بإحدى هاتين العقوبتين كل من اعترض بدون وجه حق أية معلومات أو بيانات أو كل ما هو متداول عن طريق شبكة معلوماتية أو أحد أجهزة الحاسب الألي وما في حكمها) .

2) يعاقب بالحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن 100 ألف جنيه ولا تجاوز 500 ألف جنيه، أو بإحدى هاتين العقوبتين كل من أتلّف أو عطل أو عدل مسار أو ألغى كلياً أو جزئياً، متعمداً وبدون وجه حق، البرامج والبيانات أو المعلومات المخزنة، أو المعالجة، أو المولدة أو المخلفة علي أي نظام معلوماتي وما في حكمه، أي كانت الوسيلة التي استخدمت في الجريمة) .

3) يعاقب بالحبس مدة لا تقل عن شهر، وبغرامة لا تقل عن 50 ألف جنيه ولا تجاوز 100 ألف جنيه أو بإحدى العقوبتين كل من أتلّف أو عطل أو أبطأ أو اخترق بريدًا إلكترونيًا أو موقعًا أو حسابًا خاصًا بأحد الناس. فإذا

الخاصة بالدولة¹ ، وفي المادة 21 عاقب علي جريمة الاعتداء علي سلامة الشبكة المعلوماتية
² ، وعاقب بالفصل الثاني علي الجرائم المرتكبة بواسطة أنظمة وتقنيات المعلومات وبالفصل
الرابع (الجرائم المرتكبة من مدير الموقع) ، وبالفصل الخامس (المسئولية الجنائية لمقدمي
الخدمة) .

وبناء علي ما تقدم يجب تزويد سلطات التحقيق بوحدات متخصصة تدعمها كي تستدل
علي كشف الجريمة الرقمية بأنواعها الي جانب التعاون وتبادل المعلومات ما بين الشرطة

وقعت الجريمة علي بريد إلكتروني أو موقع أو حساب خاص بأحد الأشخاص الاعتبارية الخاصة، تكون العقوبة
الحبس مدة لا تقل عن 6 أشهر وبغرامة لا تقل عن 100 ألف جنيه ولا تجاوز 200 ألف جنيه أو بإحدى هاتين
العقوبتين) .

1 (يعاقب بالحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن 50 ألف جنيه ولا تجاوز 200 ألف جنيه، أو
يأخذى هاتين العقوبتين، كل من دخل عمداً أو بخطأ غير عمدي وبقي بدون وجه حق، أو تجاوز حدود الحق
المخول له من حيث الزمان أو مستوي الدخول أو اخترق موقعا أو بريدا إلكترونيا أو حسابا خاصا أو نظاما
معلوماتيا يدار بمعرفه أو لحساب الدولة أو أحد الأشخاص الاعتبارية العامة، أو مملوك لها أو يخصها) .
فإذا كان الدخول بقصد الاعتراض أو الحصول بدون وجه حق علي بيانات أو معلومات حكومية تكون العقوبة
السجن والغرامة التي لا تقل عن 100 ألف جنيه ولا تجاوز 500 ألف جنيه" .

(وفي جميع الأحوال، إذا ترتب علي أي من الأفعال السابقة إتلاف تلك البيانات أو المعلومات أو ذلك الموقع
أو الحساب الخاص أو النظام المعلوماتي أو البريد الإلكتروني أو تدميرها أو تشويهها أو تغييرها أو تغييرها أو
تصميمها أو نسخها أو تسجيلها أو تعديل مسارها أو إعادة نشرها أو إلغائها كلياً أو جزئياً بأي وسيلة كانت، تكون
العقوبة السجن والغرامة التي لا تقل عن مليون جنيه ولا تجاوز 5 ملايين جنيه) .

2) يعاقب بالحبس مدة لا تقل عن ستة أشهر وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه
أو بإحدى هاتين العقوبتين، كل من تسبب متعمداً في إيقاف شبكة معلوماتية عن العمل أو تعطيلها، أو الحد من
كفاءة عملها، أو التشويش عليها، أو إعاقتها، أو اعتراض عملها، أو أجري بدون وجه حق معالجة إلكترونية
للبيانات الخاصة بها) .

(ويعاقب كل من تسبب بخطأ في ذلك، بالحبس مدة لا تقل عن ثلاث شهور، وبغرامة لا تقل عن خمسون ألف
جنيه ولا تجاوز مائتي الف جنيه أو بإحدى العقوبتين. فإذا وقعت الجريمة علي شبكة معلوماتية تخص الدولة أو
أحد الأشخاص الاعتبارية العامة، أو تدار بمعرفتها أو تمتلكها، تكون العقوبة السجن المشدد وبغرامة لا تقل عن
خمسمائة ألف جنيه ولا تجاوز مليون جنيه) .

والقضاء محليا ودوليا¹ ، بالإضافة إلي خطة وزارة العدل لترفع القدرات الخاصة بالقضاة ، ورؤساء المحاكم ووكلاء النيابة العامة ، من اجل تزويدها بأحدث المعلومات مما يوفر المناخ الملائم لسرعة التقاضي وإصدار الأحكام في تلك القضايا محققا بيئة رقميه آمنة للدولة لمواجهه ومكافحة ذلك النوع من الجرائم الذي أصبح منتشرا كثيرا في تلك الآونة.

5 - كما صدر مؤخرا بناءا علي مناداة فقهاء القانون والقضاء قانون رقم ١٥١ لسنة

٢٠٢٠ بإصدار قانون حماية البيانات الشخصية والمكون من 49 مادة تناول فيها المشرع ما

يلي :

وبموجب القانون الجديد سيتم إنشاء هيئة عامة اقتصادية تحت مسمى «مركز حماية البيانات الشخصية»، تكون مهمتها حماية البيانات وتنظيم معالجتها وإتاحتها لاسيما للأشخاص والشركات، وذلك برئاسة الوزير المختص وعضوية ممثل عن وزارة الدفاع يختاره وزير الدفاع، وكذا بالنسبة لوزارة الداخلية، وجهاز المخابرات العامة، وهيئة الرقابة الإدارية، وهيئة تنمية صناعة تكنولوجيا المعلومات، فضلا عن رئيسا تنفيذيا، وثلاثة من ذوي الخبرة يختارهم الوزير، علي أن تكون مدة عضوية مجلس الإدارة 3 سنوات قابلة للتجديد.

وعرف القانون البيانات الشخصية بمفهوم واسع، إذ نص علي أنها أي بيانات متعلقة بشخص طبيعي محدد، أو يمكن تحديده بشكل مباشر أو غير مباشر عن طريق الربط بين هذه البيانات

1 ولقد نص المشرع بالمادة (4) من قانون 175 لسنة 2018 الخاص بالجرائم الإلكترونية علي :

(تعمل السلطات المصرية المختصة علي تيسير التعاون بالبلاد الأجنبية في إطار الاتفاقيات الدولية والإقليمية والثنائية المصادق عليها، أو تطبيق مبدأ المعاملة بالمثل، بتبادل المعلومات بما من شأنه أن يكفل تقادي ارتكاب جرائم تقنيه المعلومات علي أن يكون المركز الفني للاستعداد لطوارئ الحاسب والشبكات بالجهاز هو المنقطة الفنية المعتمدة في هذا الشأن) .

وأى بيانات أخرى بالاسم، أو بالصوت، أو بالصورة، أو برقم تعريفى، أو محدد للهوية عبر الإنترنت، أو أى بيانات تحدد الهوية النفسية أو الصحية أو الاقتصادية أو الثقافية أو الاجتماعية. ولم يقتصر القانون علي البيانات الشخصية فحسب، بل شمل البيانات المعالجة أيضا، والتي عرفها بالعملية الرقمية أو تقنية لكتابة البيانات الشخصية، أو تجميعها، أو تسجيلها، أو حفظها، أو تخزينها، أو دمجها، أو عرضها، أو إرسالها، أو استقبالها، أو تداولها، أو نشرها، أو محوها، أو تغييرها، أو تعديلها، أو استرجاعها أو تحليلها، وذلك باستخدام أي وسيط من الوسائط أو الأجهزة الرقمية أو التقنية سواء كان ذلك بشكل جزئي أو كلي.

واشترط القانون لجمع البيانات الشخصية أو معالجتها أو الإفصاح عنها أو إفشائها بأي وسيلة من الوسائل، موافقة صريحة من الشخص المعني بالبيانات أو في الأحوال المصرح بها قانونا، كما اشترط لجمع البيانات ومعالجتها والاحتفاظ بها، توافر اربعة شروط، هي: «أن تجمع البيانات الشخصية لأغراض مشروعته ومحددة ومعلنة للشخص المعني، وأن تكون صحيحة وسليمة ومؤمنة، وأن تعالج بطريقة مشروعته وملائمة للأغراض التي تم تجميعها من أجلها، وألا يتم الاحتفاظ بها لمدة أطول من المدة الزمنية اللازمة للوفاء بالغرض المحدد لها -علي أن تحدد اللائحة التنفيذية للقانون، والتي من المقرر أن تصدر قريبا، السياسات والإجراءات والضوابط والمعايير القياسية في هذا الشأن».

ووضع القانون ضوابط عدة لمتحكمي البيانات ومعالجتها، والذي عرفهما بأنهما «أي شخص طبيعي أو اعتباري يكون له بحكم أو طبيعة عمله الحق في الحصول علي البيانات الشخصية، أو المختص بطبيعة عمله بمعالجة البيانات الشخصية»، وفي مقدمتها الحصول علي ترخيص أو تصريح من مركز حماية البيانات الشخصية، وكذا محو البيانات لديهما فور انقضاء الغرض

المحدد منها، وحال الاحتفاظ بالبيانات بالنسبة للمتحمك لأي سبب من الأسباب المشروعة بعد انتهاء الغرض، يجب ألا تبقى في صورة تسمح بتحديد الشخص المعني بالبيانات.

كما ألزم القانون معالج البيانات بعدم إجراء أي معالجة للبيانات الشخصية تتعارض مع غرض المتحمك فيها أو نشاطه، إلا إذا كان ذلك بغرض إحصائي أو تعليمي ولا يهدف للربح ودون الإخلال بحرمة الحياة الخاصة.

واشترط القانون اربعة حالات يجب أن تتوافر إحداهم للمعالجة الرقمية للبيانات حتي تكون مشروعة وقانونية، وهي: «موافقة الشخص المعني بالبيانات علي إجراء المعالجة من أجل تحقيق غرض محدد أو أكثر، وأن تكون المعالجة لازمة وضرورة تنفيذها لالتزام تعاقدى أو تصرف قانوني لإبرام عقد لصالح الشخص المعني بالبيانات، أو لمباشرة أي من إجراءات المطالبة بالحقوق القانونية له أو الدفاع عنها».

كما تضمنت الاشتراطات: «تنفيذ التزام ينظمه القانون أو أمر من جهات التحقيق المختصة أو بناءً علي حكم قضائي، أو تمكين المتحمك من القيام بالتزاماته أو أي ذي صفة من ممارسة حقوقه المشروعة ما لم يتعارض ذلك مع الحقوق والحريات الأساسية للشخص المعني بالبيانات».

وبموجب القانون بات لزاما علي جامعي ومعالجي البيانات عموما لاسيما لاستخدامات التسويق الرقمي، الحصول علي التراخيص والتصاريح والاعتمادات اللازمة لمباشرة أعمالهم، علي أن تحدد ذلك تفصيلا اللائحة التنفيذية للقانون، وذلك بمقابل رسوم مادية لا تتجاوز مليوني جنيه بالنسبة للتريخيص، ومبلغ لا يتجاوز 500 ألف جنيه للتصريح أو الاعتماد.

واستثنى القانون ستة أنواع من البيانات في تطبيق أحكامه، وهي: «البيانات الشخصية التي يحتفظ بها الأشخاص الطبيعيون للغير، والمعالجة للاستخدام الشخصي، والبيانات الشخصية التي

تتم معالجتها بغرض الحصول علي البيانات الإحصائية الرسمية أو تطبيقا لنص قانوني، والبيانات الشخصية التي تتم معالجتها حصرا للأغراض الإعلامية، إلا أن القانون انشطر في هذه الحالة أن تكون صحيحة ودقيقة، وألا تستخدم في أي أغراض أخرى، ودون الإخلال بالتشريعات المنظمة للصحافة والإعلام».

كما تضمنت قائمة الاستثناءات «البيانات الشخصية المعلقة بمحاضر الضبط القضائي والتحقيقات والدعاوي القضائية، والبيانات الشخصية لدي جهات الأمن القومي، وما تقدره لاعتبارات أخرى، والبيانات الشخصية لدي البنك المركزي والجهات الخاضعة لرقابته وإشرافه، عدا شركات تحويل الأموال وشركات الصرافة».

وألزم القانون مركز حماية البيانات، إخطار الشخص أو الجهة المتحكمة في البيانات أو المعالجة لها بتعديل أو محو أو عدم إظهار أو إتاحة أو تداول البيانات الشخصية بناءً علي طلبات جهات الأمن القومي الممثلة في رئاسة الجمهورية ووزارة الدفاع والداخلية والمخابرات العامة وهيئة الرقابة الإدارية، وذلك خلال مدة زمنية محددة وفقا لاعتبارات الأمن القومي، علي أن يلتزم المتحكم في البيانات أو المعالج لها بتنفيذ ما ورد بالإخطار خلال تلك المدة المحددة.

اللافت في القانون، أن تطبيق أحكامه لم يقتصر علي المواطنين داخل الجمهورية فحسب، بل شمل المواطنين خارج البلاد أيضا، وكذا غير المصريين المقيمين داخل الجمهورية، أو حتي خارجها، حال ما كان الفعل معاقبا عليه في الدولة التي وقع فيها تحت أي وصف قانوني، وكانت البيانات محل الجريمة لمصريين أو أجانب مقيمين داخل الجمهورية.

وأجاز القانون للمتهم المحكوم عليه لمخالفته أحكام القانون، الصلح مع المجني عليه أو وكيله الخاص أو خلفه العام، في أي حالة كانت عليها الدعوي الجنائية، شريطة أن يكون ذلك قبل

صيرورة الحكم باتا، وذلك بموافقة مركز حماية البيانات أمام النيابة العامة أو المحكمة الاقتصادية المختصة.

وألزم القانون المتهم الذي يرغب في التصالح، أن يسدد قبل رفع الدعوي الجنائية مبلغاً يعادل نصف الحد الأدنى للغرامة المقررة للجريمة، علي أن يسدد بعد رفع الدعوي وقبل صيرورة الحكم باتا نصف الحد الأقصى للغرامة المقررة للجريمة، أو قيمة الغرامة المقضي بها، أيهما أكبر، علي أن يكون السداد في خزانة المحكمة أو النيابة العامة أو المركز، ويترتب علي هذا التصالح انقضاء الدعوي الجنائية دون أن يكون له أثر في حقوق المضرور من الجريمة.

الخاتمة والنتائج

عرضنا بهذا الكتاب لموضوع الإيداع الرقمي من حيث ماهية الإيداع الرقمي بالخصوصة لقضائية ، و إجراءات المطالبة القضائية عبر الوسائط الرقمية ، وكيفية إجراء المطالبة القضائية ، وجزء النقص أو الخطأ في البيانات المقدمة بطلب عرض النزاع ، ثم عرضنا لأثار المطالبة القضائية وبيننا موقف النظم القضائية المقارنة وكذلك تناولنا أمن المعلومات من حيث المعايير الواجبة لتوافر أمن المعلومات في النظام ، و أمن المعلومات وسلامة البيانات ، ثم بيننا المخاطر التي تواجه الحق في الخصوصية في بيئة الإنترنت، والتحديات التي تواجه أنظمة التحديات التي تواجه أنظمة أمن المعلومات و إستراتيجيات أمن المعلومات Policy Security والحماية القانونية لأمن المعلومات ، وختمنا بموقف النظم القضائية المقارنة وانتهينا بناء على ما سبق عرضه إلى عدد من النتائج نعرض لها فيما يلي :

- يشهد العالم حاليا ثورة تكنولوجية هائلة مما جعلت من العالم قرية صغيرة، حيث اقتحمت وسائل الاتصال الحديثة جميع المجالات سواء في مجال العلوم أو الاتصالات أو الترفيه وغيرها الكثير جدا، وبالتالي يجب ألا يقف النظام القضائي مكتوف الأيدي أمام تلك الثورة المعلوماتية، ولابد من التحرك قدما في مجال الاستفادة من تلك الثورة الهائلة وخاصة في مجال التداعى عبر الوسائط الرقمية .
- إن التطور ليس بمنأى عن القانون، وبصفة خاصة قانون المرافعات، فهو يعد من القوانين العتيقة والتي ينبغي تطويرها بحيث يتم استخدام تكنولوجيا المعلومات في الإجراءات عموما وفي إجراءات النفاذي خصوصا ، فقدم التشريعات القائمة حاليا وعدم تماشي بعضها مع تسارع الحياة والتطورات الحديثة في التعاملات المدنية والتجارية وعدم

مواكبتها لتطورات العصر تقف حائلا أمام تلك التطورات، مما يؤدي إلي التأثير في الحياة الاقتصادية أيضا.

- خلو التشريع المصري من أي تنظيم للإيداع الرقمي بالقضاء المدني.
- اتضح من خلال تلك الدراسة أن تطبيق نظام الإيداع الرقمي ممكنا إذا تبنته إرادة سياسية وقضائية.
- نظام التقاضي الرقمي يقضي بشكل كبير جدا علي مشكلة البطء في التقاضي، مما يعمل علي تسهيل وتبسيط وتسريع إجراءات التقاضي ، و الحد من النظام الورقي، ورفع الدعوي رقميا.
- رقمية القضاء والقضاء الرقمي يشتركان في تحقيق لوجستيات التقاضي وصولاً إلي العدالة الناجزة .
- ليس المأمول من إدخال تكنولوجيا المعلومات في مجال القضاء المدني هو استبدال الآليات التقليدية للعمل القضائي بأجهزة الحاسب الآلي والبرامج اللازمة لتشغيلها، وهو ما كان يشغل بال غالبية الدول الراغبة في ميكنة نظمها القضائية.
- لا بد من تحقيق الغاية المرجوة من ذلك، وهي تفعيل أداء النظام القضائي في المجتمع، ورفع مستوى هذا الأداء . وهي الصعوبة الحقيقية التي تتحدي نجاح مثل هذه المشروعات التقنية، وليس ضعف التمويل وغياب الثقافة التكنولوجية لأفراد المجتمع فحسب.
- عدم تفاعل التشريعات النافذة مع التشريعات الحديثة العالمية والقوانين النموذجية التي صدرت عن الامم المتحدة وخاصة التشريعات الارشادية المتعلقة باستخدام الوسائل الرقمية في المعاملات المدنية والتجارية ، كالقانون الأنموذجي للتجارة الرقمية ، وكذلك

استخدامها في حل المنازعات كقواعد التحكيم الرقمي، وضرورة مواكبة تلك التغييرات التشريعية على المستويين الوطني والدولي .

■ يعتبر التقدم العلمي والتقني لكل مرافق الحياة المختلفة ، هو الطابع المميز للعصر الحديث ، وهو عنوان تقدم الدول ورفيها ، فلا بد من تطور العمل القضائي وتوصيل العدالة للمتقاضين بأيسر السبل وأسرعها ، من خلال استخدام وسائل التكنولوجيا الحديثة التي أصبحت واقعاً يجب التعامل معه ، وعدم تجاهلها او غض الطرف عنها .

■ لقد ساعد انتشار العمل بالحاسوب في كل مجالات الحياة ، ولقد سارع الكثير من مشرعي الدول الى مسايرة هذا الانتشار والتقدم التقني الى جانب تطور شبكة الاتصالات الدولية المتمثلة بالانترنت ، الى محاولة ادخال العمل به في مجال القانون ومنها امريكا وسنغافورا وانجلترا واورسترااليا ، وعلى مستوى الدول العربية الامارات ومصر والاردن والكويت والسعودية التي اتجهت فعلاً الى تطبيق نظام المحكمة الرقمية للاستفادة من التقنية الحديثة، والعراق الذي اصدر مؤخرًا قانون التوقيع الرقمي رقم (78) لسنة 2012 محاولاً تنظيم هذه الوسيلة الحديثة للاعتراف بقيمتها في ساحة القضاء .

■ يمكن تطبيق اجراءات التقاضي عبر الوسائل الرقمية لمساعدة للعنصر البشري الذي يعمل في ساحة القضاء ، لتسهيل وتبسيط وتسريع تلك الاجراءات لتحقيق مبادئ وضمانات التقاضي في ظل وجود حماية تشريعية لتلك الاجراءات تتوافق مع القواعد والمبادئ العامة التي حددها قانون المرافعات ، مع مراعاة الطبيعة الخاصة للوسائل الرقمية .

■ يمكن تطوير القواعد العامة المختصة بتطبيق اجراءات التقاضي التقليدي ، للعمل بنظام جديد اطلقنا عليه التقاضي الرقمي كما اطلقت عليه بعض التشريعات الاجنبية والعربية

، ويعتبر هذا النظام نقلة نوعية للعملية القضائية برمتها ، مع الاخذ بنظر الاعتبار ما يحتاج منها الى تدخل تشريعي بتعديلها للعمل وفق هذا النظام .

▪ يتميز نظام الإيداع الرقمي بسهولة تحرير اوراق الدعوى رقميا ، وسهولة رفعها من المدعي او وكيله ، بحيث يتم قبولها وفق الشروط التي حددها قانون المرافعات ، ويتم تسديد رسوم الدعوى بوساطة احدى وسائل الدفع الرقمية .

▪ يقلل هذا النظام الجهد المبذول في التعامل مع الوثائق وتخفيض المصاريف الادارية التي تنفقها المحكمة ، حيث ان وجود نسخة من الدعوى الرقمية على الحاسوب الخاص بالمحكمة او على دعوات رقمية يوفر كلفة تصويرها لكل من له صلة بالدعوى ،

▪ إن وجود نظام رفع الدعوى بالتقاضي عبر الوسائط الرقمية تعمل على تطبيق اجراءات التقاضي على وفق معطيات عصر التحول الرقمي ، ويؤدي الى مواكبة التطورات التي تحدث على المستوى الدولي والعالمي .

التوصيات

وبناءً علي ما تقدم ، فإننا نأمل أن يتبنى المشرع هذه التوصيات التي قد تسهم في

حلول ألمحنا إليها في ثنايا هذا الكتاب، و التي منها :

1. يجب العمل على محو الأمية الرقمية من جميع العاملين بمجال القانون والقائمين

عليه .

2. تخصيص نسبة من ميزانية الدولة متزاية للبدء فعليا في تطوير مرفق القضاء بكافة

عناصره

3. البدء في اعداد طلبة كلية الحقوق " بمرحلة الليسانس والماجستير والدكتوراه" لدراسة

مناهج تمكنهم من تطبيق التقاضي عبر الوسائط الرقمية وتطويره .

4. يجب تدريب القضاة ومعاونيهم على استخدام الوسائل الرقمية في العمل القضائي ،

على ان تكون شرط التعيين لمن يحمل شهادة (IC3) وهي اتقان العمل والمعرفة

بنظام الحاسوب ونظم الاتصالات الرقمي والانترنت .

5. يجب الاعتماد على أساليب وتقنيات متطورة للتمكن من الكشف عن هوية مرتكب

الجريمة والاستدلال عليه بأقل وقت ممكن.

6. يجب توعية الأفراد ونصحهم لماهية الجرائم الرقمية وكل ما يترتب عليها من

مخاطر.

7. يجب المسارعة في الإبلاغ للجهات الأمنية فور التعرض لجريمة رقمية.

8. يجب مواكبة التطورات المرتبطة بالجريمة الرقمية والحرص على تطوير وسائل

مكافحتها.

9. يجب استخدام برمجيات آمنة ونظم تشغيل خالية من الثغرات بالتقاضى عبر الوسائط الرقمية .
10. ضرورة إعادة صياغة النماذج والإجراءات الإدارية والقضائية رقمياً، ويندرج تحتها:
11. أ . مراعاة الملائمة بين الإجراءات القضائية والغاية من مباشرته. أي مراعاة الهدف من القيام بالإجراء القضائي.
12. ضرورة النص صراحة علي استخدام الشبكات الاجتماعية في إجراءات التحري والتقصي عن الجرائم، فهو أسلوب ناجح في التحري عن الجرائم بمعرفة الشرطة المتخصصة من خلال تحليل الشبكات لتحديد العلاقات بين المشتبه فيهم والجرائم الناشئة عن الشبكات الاجتماعية .
13. من الضروري عقد مؤتمرات دورية بين النظم القضائية المختلفة لتبادل الخبرات والتعاون المستمر في مجال تكنولوجيا المعلومات لتحديث مرفق القضاء سواء علي المستوي الداخلي أو علي المستوي الدولي.
14. ضرورة إنشاء قسمٍ جديدٍ بكليات الحقوق بالجامعات العربية لدراسة التقاضي الرقمي، وقوانين المعلوماتية، و الأمن المعلوماتي ، و معاملات العالم الرقمي.
15. ضرورة إنشاء إدارة خاصة بمواجهة الأزمات الرقمية بكل محكمة لتجنب الوقوع في الأزمات الرقمية.
16. ضرورة تبني نظام الإيداع الرقمي أمام القضاء المدني بكافة مراحل الدعوي فهو وسيلة لإقامة وقيد صحيفة الدعوي وكذا الطلبات العارضة والإدخال والتدخل

والتوقيع علي صحفها توقيعاً رقمياً معتمداً وإيداع المستندات والمذكرات والتي تتم عبر الموقع المخصص لذلك بالمحكمة المختصة لنظر الدعوي.

17. ضرورة تطوير مكاتب الحاسب الآلي بالمحاكم بحيث لا تستخدم فقط للكتابة مثل الآلة الكاتبة قديماً ، وإنما تستخدم برامج رقمية تكون اللبنة الأولى في نظام قضائي رقمي.

18. ضرورة استغلال كل الإمكانيات التي تسمح بها تكنولوجيا المعلومات والاتصالات لتحقيق غايات ميكنة إجراءات التقاضي، والقائمة علي إنجاز القضايا والفصل فيها علي وجه السرعة، وأن يذلل كافة المعوقات القانونية التي تمنع تطوير هذه الآليات الحديثة.

19. يجب صياغة القواعد القانونية المتعلقة بحماية خصوصية المعلومات المتداولة رقمياً وضمان سريتها. وهو ما يمكن أن نطلق عليه ضرورة أن يكون هناك مراجعة حقيقية، وليست سطحية أو شكلية للقواعد القانونية التي تنظم مباشرة الإجراءات القضائية عبر الوسائط الرقمية.

20. ضرورة استخدام التكنولوجيا الحديثة بالتوسع في استخدام أجهزة الحاسبات الشخصية لإمكانية مواءمتها لأي نظام معلوماتي من أي مصدر وإمكان استخدامها في أعمال آخري وتوفير أحدث وسائل وأساليب تحليل النظم وكتابة البرامج .

21. ضرورة ميكنة إجراءات النقاضي من خلال تسجيل وحفظ كافة بيانات الواردة للمحاكم .

22. يتعين وضع ملاحظات جمهور المتقاضين في الاعتبار، وخاصة تلك المتعلقة باستخدام التكنولوجيا الحديثة في النظام القضائي. فقد يتقدم المتقاضي ببعض

الملاحظات أو الاقتراحات حول أداء التقنيات التكنولوجية مما قد يؤدي إلي تحسن في أداء مرفق القضاء ككل لو أخذ القائمون علي العمل التقني بهذه الملاحظات.

وفي النهاية لا يخالجنى شك في أن هذه الدراسة المتواضعة قد اعترها بعض الأخطاء، وعذري في ذلك إنني 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 أن أردد في ذلك قوله تعالى " وما توفيقى إلا بالله " ، والشكر فيه لكل من علمني حرفاً ، وإن كانت الآخري فحسبي أن أردد في ذلك قوله تعالى "وقل رب زدني علماً" .

تم بحمد الله وفضله و توفيقه،،،،

المراجع

اولا: المراجع العربية

➤ الكتب :

- د/ رمزي سيف ، الوجيز في قانون المرافعات المدنية والتجارية المصري ، الطبعة الأولى ، مكتبة الكتب العربية ، 1957
- 1 راجع في ذلك : د/ علي بركات ، الوجيز في شرح قانون المرافعات المدنية والتجارية ، دار النهضة العربية ، 2012.
- أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، الحماية الجنائية للحاسب الآلي دراسة مقارنة ،دار النهضة العربية، الطبعة الأولى، مصر، سنة 2000
- د/ محمد حسام محمود لطفي، استخدام وسائل الاتصال الحديثة في التفاوض علي العقود وإبرامها، 1993، بدون دار نشر
- د/ وجدي راغب ، مذكرات في مبادئ القضاء المدني، 1976، بدون دار نشر
- محمود مختار، استخدام تكنولوجيا المعلومات لتيسير إجراءات التقاضي المدني ، دراسة مقارنة ، دار النهضة العربية ، ط ٢٠١٣.

➤ الرسائل العلمية :

- الباحثة هبايش فوزية ، دور التجارة الإلكترونية في تفعيل مناطق التجارة الحرة حالة منطقة التجارة الحرة العربية الكبرى، رسالة ماجستير ، جامعة حسينية بن

بوعلي بالشلف كلية العلوم الاقتصادية والتجارية وعلوم التسيير قسم العلوم الاقتصادية ، 2012.

➤ د/ قدرى محمد محمد مصطفى محمود ، حماية المستهلك في العقد الإلكتروني ، رسالة ماجستير ، جامعة القاهرة ، 2012.

➤ د/ محمد صابر احمد ، دور الحاسب الآلي في تيسير إجراءات التقاضي ، دور الحاسب الآلي في تيسير إجراءات التقاضي " ، رسالة دكتوراه ، كلية الحقوق ، جامعة طنطا ، 2012 ،

➤ الأوراق البحثية :

➤ المهندس/ سعيد عطا الله ، ما الفرق بين الأمان والخصوصية، مقال منشور بتاريخ 2020/5/14:

➤ المستشار/ ايمن رسلان ، جرائم المعلوماتية والإنترنت " بين الواقع الافتراضي والواقع بالتطبيق علي مصر والوطن العربي ، "لسنة 2012.

➤ المحامي/ يونس عرب، أمن المعلومات ماهيتها وعناصرها واستراتيجياتها ، بحث منشور علي موقع :

http://www.arablaw.org/Download/Information_Security.doc

➤ المحامي د/ يونس عرب ، جرائم الكمبيوتر والإنترنت إيجاز في المفهوم والنطاق والخصائص والصور والقواعد الإجرائية للملاحقة والإثبات ، ورقة عمل مقدمة الي مؤتمر الأمن العربي 2002 ، تنظيم المركز العربي للدراسات والبحوث الجنائية ، أبو ظبي 10-12/2/2002.

- كريستوفر كوهنر ، "متطلبات التوقيع الكتابي والمصادقة الإلكترونية: منظور مقارن" النظام المعقد للتوقيع المكتوب في القانون الألماني.
- القاضي/ حاتم جعفر ، دور التقاضي الإلكتروني في دعم وتطوير العدالة قراءة في الواقع الحالي والنتائج المتوقعة ، مؤتمر المناخ القضائي الداعم للإستثمار، الأسكندرية فبراير 2015
- القاضي د/ أسامة أحمد عبد النعيم ، " الضوابط القانونية لقرار حظر النشر ، الضوابط القانونية لقرار حظر النشر ، " الضوابط القانونية لقرار حظر النشر ، 2017.
- د/ يونس عرب ، ورقة عمل " الاتجاهات التشريعية للجرائم الإلكترونية " ، ورشة عمل " تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية " ، هيئة تنظيم الاتصالات / مسقط - سلطنة عمان ، 2 - 4 إبريل 2006
- د/ معتز السيد الزهيري ، المواجهة الجنائية لجرائم الإيذاء الإلكتروني ، بحث منشور بمؤتمر القانون والتكنولوجيا ،كلية الحقوق ، جامعة عين شمس ، ديسمبر 2017 .
- د/ محمود مختار ، بحث منشور بعنوان "الإيداع الإلكتروني" ، مؤتمر القانون والتكنولوجيا ،كلية الحقوق ، جامعة عين شمس ، ديسمبر 2017. ، الجزء الأول
- د/ محمود محمد هاشم، الخصومة أمام القضاء، بحث منشور في بعض المشكلات العملية في قانون المرافعات، إعداد مركز السنهوري للدراسات القانونية، ١٩٩٣.
- د/ محمود صالح العادلي ، الفراغ التشريعي في مجال مكافحة الجرائم الإلكترونية ، ورقة عمل.

- د/ محمد نصر القطري ، المسئولية الجنائية لوسطاء تقديم خدمات شبكة الإنترنت ، بحث مقدم للمؤتمر الدولي العاشر حول " العصر الإلكتروني وإشكالياته القانونية " ، بكلية الحقوق ، جامعة أسيوط في الفترة الممتدة من 5 إلي 6 /4/ 2016 .
- د/ فاطمة عادل سعيد ، التقاضي عبر وسائل التكنولوجيا والاتصال الحديث ، التقاضي عبر وسائل التكنولوجيا والاتصال الحديث، بحث مقدم لمؤتمر "القانون والتكنولوجيا ، كلية الحقوق ، جامعة عين شمس ، ديسمبر 2017 ، الجزء الأول.
- د/ حسن جميعي ، مدخل إلي حقوق الملكية الفكرية ، ندوة الويبو الوطنية عن الملكية الفكرية للصحفيين ووسائل الإعلام ، المنظمة العالمية للملكية الفكرية (الويبو) ، بالتعاون مع وزارة الإعلام المنامة، 16 يونيو/حزيران 2004.
- د/ جمال عبده عبد العزيز سيد الجهود الدولية لمكافحة الجرائم المعلوماتية في اطار أدلة إثباتها في التشريعات العربية ، بحث مقدم الي المؤتمر العملي الدولي الحادي عشر- لكلية الحقوق - جامعة أسيوط الاتجاهات الحديث في القانون الإجرائي ، في الفترة من 29 الي 30 مارس 2017
- د/ جبالي أبو هشيمة كامل ، حماية البيانات الشخصية في البيئة الإلكترونية دراسة مقارنة بين القانون الفرنسي ومشروع القانون المصري ، بحث منشور بمؤتمر كلية الحقوق ،جامعة أسيوط ، 2016 .
- د/ أحمد محمد عبدالرحمن ، نظرة حول نظام التقاضي الإلكتروني في مصر ، بحث مقدم للمؤتمر العلمي الحادي عشر " الاتجاهات الحديثة في القانون الإجرائي " ، كلية الحقوق ،جامعة أسيوط ، مارس 2017

➤ د/ أحمد عبد اللاه المراغي ، الجريمة الإلكترونية ودور القانون الجنائي في الحد منها ، دراسة تحليلية تأصيلية مقارنة ، بحث مقدم إلي المؤتمر العلمي العاشر لكلية الحقوق جامعة أسيوط ، " العصر الإلكتروني وإشكالياته القانونية " ، في الفترة من 5 - 6 أبريل 2016م.

➤ د / معتز السيد الزهري ، بحث بعنوان " الإيذاء عبر مواقع التواصل الاجتماعي Cyber bullying " ، بحث منشور بالمؤتمر العلمي الدولي الثاني "المجتمع العربي وشبكات التواصل الاجتماعي في عالم متغير" ، 31 أكتوبر - 2 نوفمبر 2017 ، جامعة السلطان قابوس، مسقط، سلطنة عمان

➤ د / عمر عبد العزيز الدبور ، آليات تفعيل الحماية والوقاية من الجرائم الإلكترونية (إنشاء ضبطينية خاصة بالجرائم الإلكترونية) ، بحث مقدم الى المؤتمر العملى الدولي الحادي عشر- لكلية الحقوق - جامعة أسيوط الاتجاهات الحديث في القانون الإجرائي ، فى الفترة من 29 الى 30 مارس 2017).

➤ د / إبراهيم محمد السعدي ، دور التكنولوجيا فى التغلب على ظاهرة البطء فى التقاضى، دور التكنولوجيا فى التغلب على ظاهرة البطء فى التقاضى امام القضاء المدنى فى مصر، مؤتمر القانون والتكنولوجيا ،كلية الحقوق، جامعة عين شمس ، ديسمبر 2017 ، الجزء الأول ، ص 505 وما بعدها .

➤ جمال محمد غيطاس ، الأمن المعلوماتي والجرائم الإلكترونية أدوات جديدة للصراع ، مقال منشور علي موقع مركز الجزيرة للدراسات : <https://tasharuk.net/ar/resources/index.php?id=657> ، 1 مارس

2012

- الباحث / صغير يوسف ، الجريمة المرتكبة عبر الإنترنت ، رسالة ماجستير ،
كلية الحقوق والعلوم السياسية ، جامعة مولود معمري تيزي وزو ، 2013
- الباحث / حسين خلف موسي، استراتيجية أمن المعلومات فى ظل حروب الجيل
السادس ، خاص لمركز شُرُفات لدراسات العولمة والارهاب ، عمان ،الأردن 9
مارس، 2017.
- أ.م. د/ مني تركي و م.م. جان سيريل ، الخصوصية المعلوماتية واهميتها ومخاطر
التقنيات ،مجلة كلية بغداد للعلوم الاقتصادية الجامعة العدد الخاص بمؤتمر الكلية
2013
- ا . د / عبد العزيز ملحم بربر ، امن الشبكات والإنترنت ، حلقة علمية بعنوان
الإنترنت والإرهاب ، جامعة نايف العربية للعلوم الأمنية ، 15-19/11/2008.

Book:

- AIJA ، VSCL LEGAL XML & ELECTRONIC FILING: THE AUSTRALIAN FOCUS (Melbourne (October 2001) p3 ، [http://www.aija.org.au / AIJAVSCL / AIJAVSCLtopic6.pdf](http://www.aija.org.au/AIJAVSCL/AIJAVSCLtopic6.pdf)
- Ali Rıza ÇAM، Première section une justice transparente et efficace، op. cit.، Caroline BOISSEL، e-greffe : de la dématérialisation des actes de procédure vers le développement d'une justice en ligne ?، mémoire، 2004 ؛ [www.memoireonline.com /.../m_utilisation-nouvelles-technologies-](http://www.memoireonline.com/.../m_utilisation-nouvelles-technologies-)،
- Charles Lane ،Anthrax Scare Prompts Supreme Court E-filing Discussions Washington Post 17.12.2001 ، http://www.infowar.com/law/01/law_121701c_j.shtml.
- Daniel B. Garrie, & Daniel K. Gelb, An Argument for Uniform E-Discovery Practice in Cross-Border Civil Litigation, 7 J. Bus. & Tech. L. p341-359 (2012) Available at: <http://digitalcommons.law.umaryland.edu/jbtl/vol7/iss2/4>
- Electronic Technology and Civil Procedure New Paths to Justice from Around the World : Miklós Kengyel ، Zoltán Nemessányi، (2021/1/8 : تاريخ آخر دخول علي الموقع : .
- Fabien GELINAS، Interopérabilité et normalisation des systèmes de cyber، justice : *Orientations*، www.lex-electronica.org/docs/articles_62.pdf
- Fabrice CALVET La dématérialisation et la signification des actes d'Huissiers de justice ou la plus value en matière de transmission de l'information judiciaire، mémoire، UNIVERSITE LUMIERE LYON 2، Année universitaire 2007 / 2008، www.memoireonline.com/.../m_La-dématérialisation-et-la-signification، p.30

- Kirley, Elizabeth Anne, "Reputational Privacy and the Internet: A Matter for Law?" (2015). PhD Dissertations.p 8. <http://digitalcommons.osgoode.yorku.ca/phd/8> (تاريخ آخر دخول علي) الموقع : 2021/1/8
- Kristin Finklea : Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement , January 15, 2015
- Mikl s Kengyel; Zolt n Nemess nyi; International: Electronic technology and civil procedure : new paths to justice from around the world
- Moyeda, Jessica, "Courtroom Technology" (2014), Cornell Law School Graduate Student Papers , Paper 30. http://scholarship.law.cornell.edu/lps_papers/30 (تاريخ آخر دخول) (علي الموقع : 2021/1/8)
- Osama ahmed Attalla, "is the legal protection of digital privacy enough in Egypt"? Protection of digital data privacy "
- Sophia BINET, L'utilisation des nouvelles technologies dans le procès civil : Vers une procédure civile intégralement informatisée.
- Timothy J. Chorvat and Laura E. Pelanek , Electronically Stored Information in Litigation Source, The Business Lawyer , November 2010, Vol. 66, No.1 (November 2010), pp. 183- 189 , Published by: American Bar Association Stable , URL: <https://www.jstor.org/stable/25758532>
- Yamaguchi (Atsushi): "Computer crimes and others crimes against information Technology in Japan, Rev. int. de dr. pén. 1993. P 448
- 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

- Civil Litigation in the time of Covid-19: Everything you need to know and consider www.2tg.co.uk

Sites:

- <http://www.arablaw.org>
- https://www.cc.gov.eg/civil_judgments
- http://www.bundesgerichtshof.de/BGH_ERV_Info_2001-11-20.pdf
- www.cc.gov.eg
- https://www.cc.gov.eg/civil_judgments
- <http://bo-ecli.eu/ecli/european-e-justice-portal>
- <http://braddellbrothers.com/litigation.html>
- <http://scaleplus.law.gov.au/html/pasteact/3/3328/top.htm>
- [http://www.aija.org.au / AIJAVSCL / AIJAVSCLtopic6.pdf](http://www.aija.org.au/AIJAVSCL/AIJAVSCLtopic6.pdf) >.
- <http://www.alittihad.ae/details.php?id=52871&y=2016&article=full>
- <http://www.aph.gov.au/library/pubs/bd/1999-2000/2000BD064.htm>‘
- <http://www.arablaw.org>
- <http://www.austlii.edu.au/au/journals/MurUEJL/2002/42.html>
- <http://www.austlii.edu.au/forms/search1.html>‘ FOCUS ‘ Melbourne ‘October 2001)
- <http://www.courts.state.co.us/iis/projects/efile/iisefile.htm>
- http://www.hmcourtsservice.gov.uk/onlineservices2/claim_process/make_claim.htm‘ visited 1 Desember 2019.

- <http://www.justice.gov.uk/courts/court-lists/list-companies-windingup>، last visited 9 October 2017.
- http://www.kuner.com/data/articles/signature_perspective.html
(تاريخ آخر دخول علي الموقع : 2019/12/12)
- <http://www.law.gov.au/www/securitylawHome.nsf/AllDocs/599C6BC95712D9E6C?A256B9D0016CB4B> ،OpenDocument
- <http://www.mdd.uscourts.gov/content/civil-case-opening-procedures>
- <http://www.mdd.uscourts.gov/sites/mdd/files/CivilNOSDescriptions.pdf>.
- <http://www.mdd.uscourts.gov/sites/mdd/files/SocialSecurityCasesProceduresManual.pdf>
- <http://www.singaporelaw.sg/sglaw/laws-of-singapore/overview/chapter-2> --
- <http://braddellbrothers.com/litigation.html>.-
- <http://www.singaporelaw.sg/sglaw/laws-of-singapore/overview/chapter-2>
- <http://www.uscourts.gov/cmecf/cmecf.html>
- http://www.uscourts.gov/Press_Releases/elecattach.pdf
- <http://www.worldcat.org/title/electronic-technology-and-civil-procedure-new-paths-to-justice-from-around-the-world/oclc/773670695>
- <https://customers.microsoft.com/en-us/story/adgm-azure-office365-dynamics365-uae>
- <https://docplayer.net/10015902-Summary-of-technical-information-security-for-information-systems-and-services-managed-by-nuit-newcastle-university-it-service.html> آخر (تاريخ دخول علي الموقع 2020/9/22)

- <https://docplayer.net/10464389-New-single-sign-on-options-for-ibm-lotus-notes-domino-2012-ibm-corporation.html> (تاريخ آخر دخول علي الموقع 2020/9/22)
- <https://docplayer.net/11178091-Electronic-filing-standards-implementing-e-filing-program-fourth-judicial-circuit-marion-county-general.html> (تاريخ آخر دخول علي الموقع 2020/9/22)
- <https://docplayer.net/11178265-St-bernard-parish-electronic-filing-at-the-louisiana-court-of-appeal-fourth-circuit-by-judge-roland-belsome-judge-daniel-dysart-and-dennis.html> (تاريخ آخر دخول علي الموقع 2020/9/22)
- <https://docplayer.net/11363722-Security-overview-enterprise-class-secure-mobile-file-sharing.html> (تاريخ آخر دخول علي الموقع 2020/9/22)
- <https://docplayer.net/13010656-This-working-paper-provides-an-introduction-to-the-web-services-security-standards.html> (تاريخ آخر دخول علي الموقع 2020/9/22)
- <https://docplayer.net/13164273-Secure-authentication-and-session-state-management-for-web-services.html> (تاريخ آخر دخول علي الموقع 2020/9/22)
- <https://docplayer.net/13164367-Gra-reliable-secure-web-services-service-interaction-profile-version-1-2-table-of-contents.html> (تاريخ آخر دخول علي الموقع 2020/9/22)
- <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/13788312-Principles-and-foundations-of-web-services-an-holistic-view-technologies-business-drivers-models-architectures-and-standards.html> (تاريخ آخر دخول علي الموقع 2020/9/22)

- <https://docplayer.net/13999066-Notes-on-network-security-introduction.html>(تاريخ آخر دخول علي الموقع 2020/9/22)
- <https://docplayer.net/14248162-A-decision-maker-s-guide-to-securing-an-it-infrastructure.html> 2020/9/22 تاريخ آخر دخول علي الموقع (
- <https://docplayer.net/15095840-Digital-signature-web-service-interface.html>(تاريخ آخر دخول علي الموقع 2020/9/22)
- <https://docplayer.net/15293838-The-workers-compensation-court-s-electronic-filing-system-guidelines.html>(تاريخ آخر دخول علي الموقع 2020/9/22)
- <https://docplayer.net/15798654-White-paper-securing-and-integrating-file-transfers-over-the-internet.html>(تاريخ آخر دخول علي الموقع 2020/9/22)
- <https://docplayer.net/15929126-Cpni-viewpoint-configuring-and-managing-remote-access-for-industrial-control-systems.html> تاريخ آخر دخول علي الموقع 2020/9/22 (
- <https://docplayer.net/16506977-User-instructions-welcome-to-the-clerk-s-office-electronic-filing-system.html>(تاريخ آخر دخول علي الموقع 2020/9/22)
- <https://docplayer.net/16983218-Overview-of-network-security-the-need-for-network-security-desirable-security-properties-common-vulnerabilities-security-policy-designs.html> تاريخ آخر دخول علي الموقع 2020/9/22 (
- <https://docplayer.net/17978767-Proxy-services-good-practice-guidelines.html>(تاريخ آخر دخول علي الموقع 2020/9/22)
- <https://docplayer.net/18491695-In-the-superior-court-of-fulton-c-state-of-georgia-amended-order-il-1plelventing-electronic-filing-for-civil-cases.html>(تاريخ آخر دخول علي الموقع 2020/9/22)

- <https://docplayer.net/18946782-Securing-web-services-from-encryption-to-a-web-service-security-infrastructure.html> (تاريخ آخر دخول علي الموقع 2020/9/22)
- <https://docplayer.net/3130959-Oracle-database-backup-service-secure-backup-in-the-oracle-cloud.html> (تاريخ آخر دخول علي الموقع 2020/9/22)
- <https://docplayer.net/680438-Instant-messaging-security.html> (تاريخ آخر دخول علي الموقع 2020/9/22)
- <https://docplayer.net/7568151-In-the-subordinate-courts-of-the-republic-of-singapore-epractice-direction-no-2-of-2007-request-for-digital-audio-recording-transcription-service.html> (تاريخ آخر دخول علي الموقع 2020/9/22)
- <https://docplayer.net/8406020-Model-user-guide-for-implementing-online-insurance-verification.html> (تاريخ آخر دخول علي الموقع 2020/9/22)
- https://e-justice.europa.eu/content_european_case_law_identifier_ecli-175-en.do
- <https://etc.ksu.edu.sa/ar/pages/report/main/security-risk>
- <https://file.supremecourt.gov>
- <https://news.microsoft.com/en-xm/2016/10/30/how-digital-justice-is-transforming-the-justice-system>
- <https://www.arageek.com/ما-الفرق-بين-الأمان-والخصوصية/>
- <https://www.esens.eu/content/e-document>
- <https://www.esens.eu/content/e-justice>
- <https://www.frontlinedefenders.org/ar/programme/digital-protection>
- https://www.isaca.org/credentialing/crisc?cid=sem_2002368&Appeal=sem&gclid=Cj0KCQiA0fr_BRDaARIsAABw4Eum00AOB

SaP472q11TtdPV52Hskrsfb10mSEcChmlh-
4SUQtK3I9TgaAhxlEALw_wcB

- https://www.justice.gov.uk/courts/procedure/civil/rules/part05/pd_part05b last visited on 10 October 2017.
- <https://www.lawtechnologytoday.org/2020/07/five-safety-tips-for-digital-payments/> (تاريخ آخر دخول علي الموقع 2020/9/22)
- <https://www.out-law.com/en/articles/2018/may/deal-with-data-risks-in-the-boardroom-or-pay-in-the-courtroom>
- https://www.researchgate.net/publication/251341160_The_Laws_of_Technology_and_the_Technology_of_Law (تاريخ آخر دخول علي الموقع 2020/9/22)
- <https://www.researchgate.net/publication/346579193> (تاريخ آخر دخول 2021/1/8 : علي الموقع)
- www.classic.austlii.edu.au
- www.clcio.com
- www.e-filling.com، www.maillycy.fr
- www.e-govs.com
- www.egypt.gov.eg
- www.elitigation.sg
- www.moj.gov.sa
- www.netfind.com
- www.pdfactory.com
- www.supremecourt.gov.sg

الفهرس

المبحث الأول	
الإيداع الرقمي	
14	المطلب الأول: ماهية الإيداع الرقمي بالخصومة القضائية
17	المطلب الثاني: إجراءات المطالبة القضائية عبر الوسائط الرقمية
23	الفرع الأول: كيفية إجراء المطالبة القضائية
26	الفصل الأول: البيانات الواجب توافرها في الطلب المقدم عبر إجراءات التقاضي الرقمي
29	الفصل الثاني: المتطلبات الأخرى لقبول طلب رفع الدعوى رقمياً
34	الفرع الثاني: جزاء النقص أو الخطأ في البيانات المقدمة بطلب عرض النزاع
37	المطلب الثالث: آثار المطالبة القضائية
43	المطلب الرابع: موقف النظم القضائية المقارنة
المبحث الثاني	
أمن المعلومات	
64	المطلب الأول: معايير أمن المعلومات وسلامة البيانات
65	الفرع الأول: المعايير الواجبة لتوافر أمن المعلومات في النظام
69	الفرع الثاني: أمن المعلومات وسلامة البيانات

80	المطلب الثانى : المخاطر التي تواجه الحق في الخصوصية في بيئة الإنترنت
87	المطلب الثالث : التحديات التي تواجه أنظمة أمن المعلومات واستراتيجياتها والحماية القانونية
88	الفرع الأول : التحديات التي تواجه أنظمة أمن المعلومات
102	الفرع الثانى : إستراتيجيات أمن المعلومات Security Policy
122	الفرع الثالث : الحماية القانونية لأمن المعلومات
124	المطلب الرابع : موقف النظم القضائية المقارنة
125	الفرع الأول : موقف التشريعات الغربية
128	الفرع الثانى : موقف التشريعات العربية
140	الخاتمة و النتائج
144	التوصيات
148	المراجع

