(ISSN: 2356 - 9492)

عنوان الورقة البحثية

دور الدول في الحماية القانونية للبيانات الشخصية في عصر التقاضي الإلكتروني

"دراسة مقارنة"

د/ ريم جمعه ذكري

أستاذ مساعد بكلية الخليج

reemzekry89@gmail.com

201064643586

المستخلص:

يتناول هذا البحث إشكالية حماية البيانات الشخصية في ظل التوسع المتسارع للتقاضي الإلكتروني، خاصةً في ضوء إمكانية جمع ونقل كميات كبيرة من المعلومات الحساسة للأفراد كجزء من الإجراءات القضائية الرقمية. في ظل التهديدات المتزايدة للانتهاكات الأمنية والقرصنة، يصبح توفير حماية قانونية فعالة لهذه البيانات ضرورة ملحة، انطلاقًا من الحق الأساسي للإنسان في الحفاظ على خصوصيته وحماية معلوماته من الاستخدام غير المشروع. تكمن أهمية البحث في إجراء دراسة مقارنة بين التشريعات المصرية والسعودية في مجال حماية البيانات الشخصية وجرائم تقنية المعلومات، بالإضافة إلى استعراض الاتفاقيات الدولية ذات الصلة، خاصةً مع التحول الرقمي الكبير في نظام التقاضي السعودي. يسعى البحث للإجابة عن التساؤلات المتعلقة بمدى كفاية القوانين الحالية لمواكبة التطورات التكنولوجية وتوفير الحماية اللازمة للبيانات المتحصل عليها عبر التقاضي الإلكتروني. ولتحقيق ذلك، يعتمد البحث على المنهج الوصفي التحليلي للقوانين والمعاهدات ذات الصلة، ويقترح خطة بحثية تتناول مفهوم التقاضي الإلكتروني والضمانات القانونية الضرورية لحماية البيانات الشخصية للأفراد في هذا السياق.

الكلمات المفتاحية: حماية البيانات – البيانات الشخصية – التقاضي الإلكتروني – العدالة الإلكترونية

(ISSN: 2356 - 9492)

Abstract:

This research addresses the critical issue of personal data protection considering the rapidly expanding adoption of electronic litigation, particularly considering the potential for the collection and transfer of substantial amounts of sensitive personal information as part of digital judicial procedures. Given the increasing threats of security breaches and hacking, providing effective legal safeguards for this data has become an urgent necessity, stemming from the fundamental human right to privacy and the protection of personal information from unauthorized use. The significance of this research lies in conducting a comparative study between Egyptian and Saudi Arabian legislation in the field of personal data protection and cybercrime, in addition to reviewing relevant international agreements, especially with the significant digital transformation in the Saudi Arabian judicial system. This study seeks to answer questions regarding the adequacy of current laws to keep pace with technological advancements and provide the necessary protection for data obtained through electronic litigation. To achieve this, the research employs a descriptive-analytical approach to relevant laws and treaties and proposes a research plan that examines the concept of electronic litigation and the essential legal guarantees for safeguarding individuals' personal data in this context.

Keywords: Data protection, Personal data, E-litigation, electronic justice.

المقدمة

الحمد لله رب العالمين، والصلاة والسلام على أشرف خلق الله أجمعين سيدنا محمد صلى الله عليه وسلم أما بعد. في ظل التطور التكنولوجي المجتاح للعالم بقوة ولكل المجالات العلمية والعملية بما في ذلك المجال القانوني والقضاء.

وفي ضوء أن القضاء قد يجبر الأفراد على تقديم الكثير من معلوماتهم كأدلة ومستندات دونما موافقة منهم في بعض الأحيان. وعلى مدار رفع الدعوى الإلكترونية لحين الفصل فيها كالبيانات الشخصية والمستندات الخاصة بالدعوى وبيانات الخصم الشخصية وخلافه. ورقمنه تلك البيانات وجعلها كجزء من قاعدة المعلوماتية للدولة التي قد تتعرض للانتهاكات والقرصنة في يوم ما. وعلى ذلك كان لابد أن يكون هناك نوع من أنواع الحماية القانونية لتلك البيانات لسهولة قرصنتها والاستيلاء عليها. وذلك لأن من حقوق الإنسان الرئيسية هو حقه في الحفاظ على معلوماته الشخصية وحمايتها، بل وحمايته من استعمالها بطريقة غير مشروعة.

تكمن أهمية الموضوع في وجود دراسة مقارنة بين القوانين المختلفة للدول وخصوصا القانون المصري والسعودي في مجال حماية البيانات الشخصية والعقوبات المقررة في الجرائم المعلوماتية في كلا البلدين والاتفاقيات الدولية. خصوصا في ظل التطور التكنولوجي الرهيب وأن الأساس في التقاضي في المملكة العربية السعودية أصبح الكترونيا في غالب الدعاوي. وكذلك مدى تأثر حقوق الإنسان المقررة وفقا للقانون والاتفاقيات الدولية.

بينما تتمثل إشكالية البحث في حداثة التقاضي الإلكتروني وكذلك البيانات المتحصل عليها عن طريقة وكيفية حماية تلك البيانات في ظل التطور التكنولوجي الرهيب، وكذلك عدم مواكبة القوانين لهذه التطورات بذات السرعة المطلوبة. مما أدى إلى قلة الأبحاث والكتب الموجودة في هذا المجال.

ولقد اعتمدت على المنهج الوصفي التحليلي للقوانين المختلفة والمعاهدات في مجال حماية المعلوماتية وكذلك التقاضي الإلكتروني.

(ISSN: 2356 - 9492)

كما يمكن تقسيم خطة الورقة البحثية إلى ثلاثة أجزاء أولا سأتحدث عن التقاضي الإلكتروني بينما في ثانيا سأتحدث عن الضمانات القانونية التي يجب توافرها لحماية البيانات الشخصية للأفراد. وفي النهاية سأختتم بمقارنة موجزة بين قوانين حماية البيانات الشخصية في مصر، الإمارات، المغرب، والسعودية

وذلك على النحو الآتي.

أولا: التقاضي الإلكتروني:

لقد تعددت تعريفات الفقهاء للتقاضي الإلكتروني. فلقد عرف بعض الفقهاء التقاضي الإلكتروني بأنه "سلطة لمجموعة من القضاة النظاميين بنظر الدعوى ومباشرة الإجراءات القضائية بوسائل إلكترونية مستحدثة، ضمن أنظمة قضائية معلوماتية متكاملة الأطراف والوسائل تعتمد على تقنية شبكات الإنترنت وبرامج الملفات الحاسوبية الإلكترونية بنظر الدعاوي والفصل فيها وتنفيذ الأحكام وذلك بهدف الوصول لفصل سريع في الدعاوي و للتسهيل على المتقاضين[١]" بينما عرفه آخرون بأنه "سلطة المحكمة القضائية المتخصصة للفصل إلكترونيا بالنزاع المعروض أمامها من خلال شبكة الربط الدولية وبالاعتماد على أنظمة إلكترونية وآليات تقنية فائقة الحداثة بهدف سرعة الفصل في الخصومات والتسهيل على المتخاصمين"[٢]. مما سبق يمكن أن نعرف التقاضي الالكتروني بأنه " نظام قضائي يمكن للمتقاضين عن طريقه رفع الدعاوي إلكترونيا مستخدمين في ذلك وسائل التقنية الرقمية ابتداء من رفع الدعوى حتى تنفيذ الحكم الصادر فيها إلكترونيا، وذلك بهدف سرعة الفصل في الدعاوي وتسهيل الإجراءات على المتقاضين".

من التعريفات السابقة يمكن لنا استخلاص خصائص التقاضي الإلكتروني وما يتميز به. إن أول مميزات هذا النظام أنه تم الاعتماد على التقنية الرقمية في كافة إجراءاته دونما استخدام للملفات الورقية، بل يكمن تميزه في السجلات الرقمية التي يمكن الوصول إليها والاطلاع عليها بكل سهولة. كما يتميز كذلك في سهولة ومرونة الإجراءات مما يؤدي إلى اختصار الوقت والجهد وذلك بالقضاء على البيروقراطية والتعقيد في الإجراءات التقليدية لرفع الدعوى[٣]. هذا بالإضافة إلى سرعة اتخاذ الإجراءات القضائية وكذلك سرعة البت في القضايا وتنفيذها وذلك لأن جميع إجراءات رفع

الدعوى أصبحت تتم عبر تطبيق الكتروني وبخطوات بسيطة. كل ما سبق ذكره من خصائص يؤدي إلى تحقيق كفاءة وفاعلية الجهاز القضائي في الدولة بأكملها. وفي النهاية فإن الحد من التدخل البشري بما تعتريه من ضعف نفس أو إهمال أو تلاعب والاعتماد على القضاء الرقمي يؤدي إلى زيادة الشفافية ومكافحة الفساد[١].

ولضمان نجاح التقاضي الإلكتروني لابد من توافر بعد المتطلبات ومنها أولا أن يكون قد صدر تشريع يجيزها بدءا من إيداع صحيفة الدعوى حتى وجود توقيع إلكتروني للأحكام تنفيذها. كذلك أن يكون لهذه المحاكمات نظام إلكتروني خاص بها من برامج معلوماتية وأدوات تقنية لتخزين البيانات والمعلومات عن طريق هيئة تقوم بإنشاء موقع الكتروني للمحكمة وربطه بأجهزة الحكومية الإلكترونية كافة وتنظيمه لتنسيق القضايا والمستندات والأدلة الخاصة به. كما إنه لابد من تحديد آلية فعالة لعقد الجليات عن بعد مثل team, zoom, web box وخلافه. كما إنه يجب تحديد المصرح لهم بدخول تلك المحاكمات[٢]. كذلك لابد من تنظيم آلية خاصة بالتحقق من شخصية أطراف الخصومة وكيفية تسجيلهم هم ومستنداتهم وتحديد رسوم الدعوى. وحتى يتم تحقيق ما سبق لابد من أن يكون هناك بنية تحتية الكترونية قوية عن طريق توفير العدد المناسب من الأجهزة والبرامج، وتوفير شبكة اتصالات مناسبة قادرة على الربط بين الجهات المختلفة بفاعلية، توفير عدد كاف من التقنيين والخبراء الفنيين في مجال علوم الحاسب تحسبا لأي عطل أو خلل كذلك لتطوير المحاكمات باستمرار[٣]، تدريب القضاة والعاملين في المحكمة الإلكترونية على استخدام الأجهزة الإلكترونية والبرامج المصاحبة لها في تطبيق المحاكمة عن بعد. وإنشاء محررات إلكترونية تستخدم كبديل للورقية ويسهل استخدامها ويسل التوقيع الإلكتروني عليها إلكترونيا. تسجيل بريد إلكتروني لكل المتعاملين مع التقاضي الإلكتروني يرتبط ببطاقة تحقيق الهوية. وفي النهاية وضع ضمانات كافية لحماية خصوصية المعلومات المستندات وهذا ما سأتناوله بالتفصيل[٤].

---

[٢] هذه الجزئية تخالف مبدأ علانية الجلسات حيث إنه ليس مصرح للجميع بدخول الجلسات، بل تقتصر على أطراف الخصومة فقط وبذلك يخل بأحد أسس التقاضي.

(ISSN: 2356 - 9492)

ثانيا: الضمانات القانونية التي يجب توافرها لحماية البيانات الشخصية للأفراد.

حيث إن المتقاضين سواء في القضاء العادي أو الإلكتروني يضحون بالعديد من المعلومات الشخصية قد تصل لتحديد ممتلكاتهم وأرقام حساباتهم البنكية. هذه المعلومات التي قد تعرض حياتهم أو ما يمتلكون لخطر العبث بها وتشويهها. لذلك يتطلب الأمر قدر كبير من الأمن السيبراني لحماية تلك الخصوصية. فالحق في الخصوصية المعلوماتية أحد الحقوق المرتبطة بشخصية الإنسان والتي نصت عليها العديد من المعاهدات الدولية والقوانين بأكملها على اختلاف أنظمتها.

ومن أنواع البيانات التي يجب حمايتها والتي وضحتها بالمجمل المادة الأولى من قانون حماية البيانات الشخصية المصري رقم ١٥١ الصادر في ٢٠٢٠ بأنها البيانات المتعلقة بشخص محدد أو يمكن تحديده بطريقة مباشرة أو غير مباشرة مثل كرقم الهاتف أو رقم السيارة أو البريد الإلكتروني. والربط بين تلك البيانات وبيانات أخرى كالاسم، أو الصوت، أو الصورة، أو رقم تعريفي، أو محدد لهوية عبر الإنترنت. أو أي بيانات تحدد الهوية النفسية، أو الصحية، أو الاقتصادية، أو الثقافية، أو الاجتماعية[١].

ويمكن الاعتداء على تلك البيانات بطرق منها التزوير الالكتروني والتي تعني تغيير الحقيقة في المحررات والوثائق الإلكترونية المقدمة للمحكمة، أو الدخول إلى نظام المحكمة من الأشخاص غير المسموح لهم بذلك للحصول على معلومات هذا النظام، أو ممكن أن يتم عن طريق تدمير او إتلاف المعلومات حتى لا يستفاد منها، كذلك ممكن أن يتم بالتلاعب في بيانات شبكة المحكمة الإلكترونية. لذلك وضعت الدول العديد من القوانين لحماية وتنظيم التقاضي عن بعد، ومعلومات وبيانات الأشخاص الخاضعين لها[٢].

ولحماية تلك البيانات اجتهدت المعاهدات والمواثيق والدول بوضع تشريع خاص بالتقاضي الالكتروني وكيفية حماية المعلومات فيه مثل المفوضية الأوروبية وإقرارها لميثاق الأخلاق الأوروبي بشأن استخدام الذكاء الاصطناعي في النظم القضائية وبيئتها، في ستراسبورغ ٢٠١٨ في مبدأه الثالث الجودة والأمان الذي نص على إنه حتى يمكن تحقيق

الجودة والأمان في التقاضي الإلكتروني و لضمان معالجة القرارات القضائية والبيانات بشكل آمن وعادل، يجب الالتزام بما يلي: أولا التعاون بين العديد من التخصصات في تصميم التقاضي الإلكتروني مثل : إشراك خبراء العدالة والقانون والعلوم الاجتماعية في ذلك. ثانيا تشكيل فرق متعددة التخصصات وعقد دورات تدريبية للعاملين لتعزيز الكفاءة. ثالثا تعزيز الضوابط الأخلاقية عن طريق مشاركة التدابير الأخلاقية بشكل مستمر وتحسينها بناءً على التغذية الراجعة. رابعا تتبع العمليات: التأكد من أن البيانات المستخدمة معتمدة وقابلة للتتبع لضمان عدم التعديل غير المصرح به أو التلاعب بها. خامسا الأمان الرقمي وذلك عن طيق تخزين وتنفيذ النماذج في بيئات آمنة لضمان سلامة النظام وسلامة البيانات. وفي ضوء ذلك المبدأ وضعت العديد من الدول قوانينها[١].

فمثلا مصر والتي طورت من منظومة التقاضي الإلكتروني وربطته بكل الجهات الحكومية. قامت بتأمين البيانات والمستندات عن طريق تشفير جميع البيانات الحساسة الخاصة بالمتقاضين بطريقة قوية لا يمكن فك تشفيرها إلا من قبل الأشخاص المخولين لهم بذلك كما وضعت جدران حماية نارية قوية لحماية أنظمة التقاضي الإلكتروني من الهجمات الإلكترونية كذلك قامت باستخدام أنظمة متطورة للكشف عن أي محاولات للتسلل للنظام أو الوصول غير المصرح به إلى البيانات قامت بتطبيق إجراءات صارمة للتحقق من هوية المستخدمين قبل السماح لهم بالوصول للنظام مثل التوقيع الإلكتروني والمصادقة الثنائية. تم عمل نسخ احتياطي للبيانات بطريقة منتظمة لضمان عدم فقدانها في حالة حدوث عطل أو كارثة كما قام بتدريب العاملين على النظام وكيفية التعامل معهم بشكل آمن. ووضعت العديد من القوانين واللوائح الصارمة التي تجرم أي انتهاك لخصوصية البيانات مع وضع عقوبات مشددة للمخالفين والتي قسمتها على حسب المخالف والمنتهك.[٢]

وكذلك دولة الإمارات العربية المتحدة والتي تعد من الدول الرائدة في مجال التقاضي الالكتروني نصت على العديد من وسائل الحماية لخصوصية معلومات ومستندات المتقاضين في المحاكمة عن بعد مثل أن تخضع المحاكمة إلى القوانين المنظمة لسياسات أمن المعلومات المعتمدة من الدولة[٣]، وأن تكون جلسات التحقيق وخصوصا الجزائية سرية،

(ISSN: 2356 - 9492)

أن يكون دخول الوكلاء والخصوم إلى نظام الجلسة عن بعد وكذلك للاطلاع على المستندات والملفات المرتبطة بدعواهم برقم سري مشفر يرسل من مكتب إدارة الدعوى بالمحكمة، أن جميع إجراءات المحاكمة عن بعد يتم تسجيلها وحفظها في نظام المعلومات الالكتروني للمحكمة وتتمتع بالسرية فلا يجوز تداولها ولا الاطلاع عليها إلا بإذن قضائي[١]، تزويد المحامين بوسيلة التواصل الرسمية الالكترونية للمحكمة المختصة بدعواه ويقوم هو أيضا بمنحهم بريده الإلكتروني، أن المداولة بين القضاة تكون على موقع إلكتروني مؤمن سيبرانيا وخاص فقط بالمداولات بين القضاة ولا يجوز لغير القضاة الولوج إليه، وفي النهاية وضع المشرع الإماراتي أن تواقيع القضاة وكتبة الجلسات تكون الكترونية وترفع في أول كل عام قضائي على النظام الإلكتروني المعلوماتي للمحكمة[٢].

بينما في دولة المغرب وضعت عدة قوانين للحماية القانونية لتلك البيانات أحداها القانون رقم٠٥-٣٥[٣] يتعلق بالتوقيع الإلكتروني المعتد أمام المحاكم وإنه لابد من الحصول من مصادقة على هذا التوقيع، بل واهتم أيضا بالتبادل الإلكتروني للأدلة والمستندات ومعطيات الدعوى بين الخصوم وبعضهم البعض وبين الخصوم والمحكمة، بل وكيفية التشفير لكل ما سبق والمخالفات الجنائية والعقوبات الموقعة في حال ارتكاب أحد تلك الجرائم، كذلك القانون رقم ٠٣-٠٧[٤] المتعلق بالجرائم التي ترتكب حال اختراق نظام المحكمة عن بعد مثل الدخول أو البقاء غير المشروع في نظام المحكمة دون تصريح بذلك، وتم تشديد العقوبة إن نتج عن هذا الدخول تغيير أو حذف أو تشويه او إضافة للمعلومات والمستندات والأدلة الموجودة والخاصة بالدعوى، كما قام بوضع جريمة التزييف والتزوير المعلوماتي. كما أن هناك القانون رقم ٠٩-٠٨[٥] والذي أهتم بكيفية حماية معلومات المتقاضين وأسند تلك المهمة إلى اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي. كذلك جرم الولوج دون وجه لأنظمة المعالجة الالكترونية للمواقع الإلكترونية المختلفة الخاصة بالتقاضي الالكتروني وذلك في القانون الجنائي المغربي.

بينما المشرع السعودي وبحق يعد من الدول المتطورة في مجال التقاضي الإلكتروني أيضا. فمثلا وضع نظام حماية للبيانات الشخصية وهو عدم استخدام تلك البيانات وسريتها إلا لأغراض محددة ولابد من موافقة الأطراف المعنية. كذلك وضع قانون لنظام مكافحة الجرائم المعلوماتية. كما إنه يعترف بالمحررات الإلكترونية والتوقيعات الرقمية. يعتمد على نظام تشفير حديث لحماية المستندات القضائية وبيانات المتقاضين من التلاعب أو الاختراق. كما يستخدم بروتوكولات اتصال آمنة مثل TLS، SSL التي تستخدم لحماية البيانات. كما إنه يعمل بنظام التعاملات الإلكتروني فاعترف بالتوقيع الإلكتروني لإثبات الهوية والاعتماد على شهادات رقمية صادرة من المركز الوطني للتصديق الرقمي. كما إنه قيد الوصول إلى منصات التقاضي الإلكتروني بوسائل تحقق مثل المصادقة الثنائية. فعل أنظمة كشف ومنع الاختراقات لحماية البنية التحتية. وفرض عقوبات مشددة على الجهات والأفراد الذين يرتكبون الجرائم المعلوماتية. كما قام بتدريب القضاة والعاملين في المحاكم الإلكترونية. وطور منصة إلكترونية تابعة لوزارة العدل مثل بوابة ناجز[1]

ثالثا: مقارنة بين نصوص قوانين حماية البيانات الشخصية في مصر، الإمارات، المغرب، والسعودية

أ: الإطار التشريعي والتعاريف الأساسية

مصر: القانون رقم ١٥١ لسنة ٢٠٢٠ بشأن حماية البيانات الشخصية

المادة:(1) البيانات الشخصية: كل بيان أيا كان مصدره أو شكله يمكن أن يؤدي إلى تحديد شخص طبيعي معين بذاته أو يمكن التعرف عليه بشكل مباشر أو غير مباشر عن طريق الربط بين هذه البيانات وأي بيانات أخرى".

المادة:(2) معالجة البيانات: أي عملية أو مجموعة عمليات تجرى على البيانات الشخصية باستخدام وسائل إلكترونية أو غير إلكترونية، مثل الجمع، أو التسجيل، أو الحفظ، أو التخزين، أو التعديل، أو التحديث، أو الاسترجاع، أو الاستخدام، أو الإفشاء، أو النقل، أو الإتاحة، أو الحذف، أو الإتلاف".

(ISSN: 2356 - 9492)

المادة:(3) البيانات الحساسة: البيانات التي تكشف عن الأصل العرقي، أو الآراء السياسية، أو المعتقدات الدينية، أو الفلسفية، أو الانتماء النقابي، أو البيانات الجينية أو البيومترية أو الصحية أو المتعلقة بالحياة الجنسية".

الإمارات: المرسوم بقانون اتحادي رقم ٤٥ لسنة ٢٠٢١ بشأن حماية البيانات الشخصية

المادة:(1) البيانات الشخصية: أية بيانات تتعلق بشخص طبيعي محدد أو قابل للتحديد بشكل مباشر أو غير مباشر، من خلال الربط مع بيانات أخرى".

المادة:(7) البيانات الحساسة: البيانات التي تكشف عن الأصل العرقي، أو الإثني، أو الآراء السياسية ،أو المعتقدات الدينية أو الفلسفية أو الانتماء النقابي أو البيانات الوراثية أو البيومترية أو الصحية أو البيانات المتعلقة بالحياة الجنسية أو البيانات المتعلقة بالأطفال أو البيانات المالية".

المغرب: القانون رقم ٠٩-٠٨ المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي

المادة:(1) المعطيات ذات الطابع الشخصي: كل معلومة كيفما كان نوعها وأيا كان سندها، بما في ذلك الصوت والصورة، والمتعلقة بشخص ذاتي معرف أو قابل للتعريف".

المادة:(22) يمنع معالجة المعطيات ذات الطابع الشخصي التي تكشف عن الأصل العرقي أو الإثني أو الآراء السياسية أو الفلسفية أو الدينية أو الانتماء النقابي أو التي تهم الحياة الجنسية للأشخاص، إلا في حالات خاصة وبترخيص من اللجنة الوطنية".

السعودية: نظام حماية البيانات الشخصية (الصادر بالمرسوم الملكي رقم م/١٩ بتاريخ ١٤٤٣/٢/٩هـ)

المادة:(1) البيانات الشخصية: كل بيان مهما كان مصدره أو شكله من شأنه أن يؤدي إلى معرفة شخص بشكل مباشر أو غير مباشر".

المادة:(4) البيانات الحساسة: البيانات التي تتعلق بالعقيدة الدينية، أو الأصل العرقي، أو الآراء السياسية، أو الانتماء الفكري، أو الوراثي، أو الصحي، أو الجنسي، أو الموقع الجغرافي، أو البيانات المالية".

ب: شروط جمع ومعالجة البيانات الشخصية

مصر

المادة:(4) لا يجوز جمع البيانات الشخصية أو معالجتها أو الإفصاح عنها أو الإفشاء عنها إلا بموافقة صريحة من الشخص المعني بالبيانات أو في الأحوال التي يحددها هذا القانون".

المادة:(6) يجب أن تكون موافقة الشخص المعني بالبيانات صريحة ومحددة وسهلة السحب في أي وقت".

الإمارات

المادة:(5) لا يجوز جمع أو معالجة البيانات الشخصية إلا بناءً على موافقة صريحة من صاحب البيانات، أو إذا اقتضت الضرورة لتنفيذ عقد أو التزام قانوني أو لحماية مصالح حيوية".

المادة:(8) يجب الحصول على موافقة صريحة ومكتوبة عند معالجة البيانات الحساسة".

المغرب

المادة:(4) يجب على المسؤول عن المعالجة أن يحصل على موافقة صريحة من الشخص المعني قبل جمع أو معالجة معطياته ذات الطابع الشخصي".

المادة:(5) يجوز معالجة المعطيات دون موافقة إذا كانت ضرورية للوفاء بالتزام قانوني أو لتنفيذ عقد يكون الشخص المعني طرفا فيه أو لحماية مصلحة حيوية".

السعودية

المادة:(5) لا يجوز جمع البيانات الشخصية أو معالجتها أو الإفصاح عنها إلا بموافقة صريحة من صاحب البيانات أو في الحالات المنصوص عليها نظاماً".

المادة:(6) يجب أن تكون الموافقة محددة وواضحة وقابلة للإثبات، ويجوز لصاحب البيانات سحبها في أي وقت".

(ISSN: 2356 - 9492)

ج: حقوق الأفراد (أصحاب البيانات)

حق الوصول

مصر (المادة ٨): لصاحب البيانات الحق في الحصول على نسخة من بياناته الشخصية لدى أي جهة خلال مدة لا تتجاوز سبعة أيام عمل".

الإمارات (المادة ١٣): يحق لصاحب البيانات طلب نسخة من بياناته الشخصية، وعلى الجهة المعالجة الاستجابة خلال خمسة عشر يوم عمل".

المغرب (المادة ٧): يحق لكل شخص أن يطلب من المسؤول عن المعالجة إعلامه بمعالجة معطياته الشخصية والحصول على نسخة منها".

السعودية (المادة ٨): يحق لصاحب البيانات طلب الوصول إلى بياناته الشخصية وتصحيحها أو حذفها خلال مدة لا تتجاوز عشرة أيام عمل".

حق التصحيح والحذف

مصر (المادة ٩): يحق لصاحب البيانات تصحيح أو حذف بياناته الشخصية إذا كانت غير صحيحة أو انتهى الغرض من معالجتها".

الإمارات (المادة ١٤): يحق لصاحب البيانات طلب تصحيح أو حذف بياناته الشخصية إذا كانت غير دقيقة أو لم يعد هناك حاجة لمعالجتها".

المغرب (المادة ٨): يحق لكل شخص أن يطلب تصحيح أو حذف معطياته الشخصية إذا ثبت أنها غير صحيحة أو غير قانونية".

السعودية (المادة ٩): يحق لصاحب البيانات طلب تصحيح أو إتلاف بياناته الشخصية إذا كانت غير صحيحة أو انتهت الحاجة منها".

حق الاعتراض وطلب التقييد

مصر (المادة ١٠): يحق لصاحب البيانات الاعتراض على معالجة بياناته الشخصية أو طلب تقييدها في حالات معينة".

الإمارات (المادة ١٥): يحق لصاحب البيانات الاعتراض على معالجة بياناته الشخصية لأسباب تتعلق بوضعه الخاص".

المغرب (المادة ٩): يحق لكل شخص الاعتراض على معالجة معطياته الشخصية إذا كانت المعالجة لأغراض تسويقية أو إذا كانت غير مشروعة".

السعودية (المادة ١٠): يحق لصاحب البيانات الاعتراض على معالجة بياناته الشخصية إذا تعارضت مع مصالحه أو حقوقه".

د: التزامات الجهات المعالجة ومسؤول حماية البيانات

تعيين مسؤول حماية البيانات(DPO)

مصر (المادة ١٨): تلتزم الجهات المعالجة بتعيين مسؤول حماية بيانات إذا كانت تعالج بيانات حساسة أو بكميات كبيرة".

الإمارات (المادة ١٠): يجب على الجهة المعالجة تعيين مسؤول حماية بيانات إذا كانت معالجة البيانات تشكل خطراً مرتفعاً على حقوق الأفراد".

المغرب لا يوجد نص صريح يلزم بتعيين مسؤول حماية بيانات، لكن اللجنة الوطنية توصي بذلك في بعض الحالات.

(ISSN: 2356 - 9492)

السعودية (المادة ١١): تلتزم الجهة المعالجة بتعيين مسؤول حماية بيانات إذا تجاوز عدد أصحاب البيانات خمسين ألف شخص".

الإبلاغ عن خروقات البيانات

مصر (المادة ١٩): يجب على الجهة المعالجة إخطار مركز حماية البيانات وأصحاب البيانات خلال اثنين وسبعين ساعة من اكتشاف أي خرق أمني".

الإمارات (المادة ١٢): يجب الإبلاغ عن أي خرق للبيانات الشخصية للسلطة المختصة خلال ثمان وأربعين ساعة ولأصحاب البيانات خلال أربعة عشر يوماً".

المغرب (المادة ٢٣): يجب على المسؤول عن المعالجة إخطار اللجنة الوطنية وأصحاب البيانات فور اكتشاف خرق أمني".

السعودية (المادة ١٢): يجب على الجهة المعالجة إخطار الهيئة وأصحاب البيانات خلال أربع وعشرين ساعة من اكتشاف الخرق".

هـ: نقل البيانات عبر الحدود

مصر (المادة ١٤): لا يجوز نقل البيانات الشخصية خارج جمهورية مصر العربية إلا بتصريح من مركز حماية البيانات وبعد التأكد من وجود مستوى حماية مناسب في الدولة المستقبلة".

الإمارات (المادة ٢٢): لا يجوز نقل البيانات الشخصية خارج الدولة إلا إذا كانت الدولة المستقبلة توفر مستوى حماية مكافئ أو بناءً على موافقة صريحة من صاحب البيانات".

المغرب (المادة ٤٣): يمنع نقل المعطيات ذات الطابع الشخصي إلى دولة أجنبية إلا إذا حصل المسؤول عن المعالجة على ترخيص من اللجنة الوطنية أو إذا كانت الدولة المستقبلة تضمن مستوى حماية كاف".

السعودية (المادة ١٤): لا يجوز نقل البيانات الشخصية خارج المملكة إلا إذا كانت الدولة المستقبلة توفر مستوى حماية لا يقل عما هو مقرر في النظام، أو بموافقة الهيئة".

و: العقوبات والجزاءات

مصر (المواد ٢٦-٢٩):

- غرامات مالية تبدأ من ١٠٠ ألف جنيه وتصل إلى ٥ ملايين جنيه.
- الحبس لمدة تصل إلى ٣ سنوات في حالات معالجة البيانات الحساسة دون تصريح.

الإمارات (المادة ٢٤):

- غرامات مالية تصل إلى ١٠ ملايين درهم.
- إغلاق المنشأة أو تعليق النشاط في حال التكرار أو المخالفات الجسيمة.

المغرب (المواد ٥٧-٦١):

- غرامات مالية تصل إلى ٣٠٠ ألف درهم مغربي.
- الحبس من شهر إلى سنة في حالات معينة.

السعودية (المادة ٢٩):

- غرامات مالية تصل إلى ٥ ملايين ريال سعودي.
- تعليق أو إلغاء الترخيص في حال تكرار المخالفة.

ز: خصوصية التقاضي الإلكتروني

(ISSN: 2356 - 9492)

تلزم جميع القوانين الجهات القضائية المختلفة والجهات الإدارية التي تدير منصات التقاضي الإلكتروني بحماية سرية البيانات الشخصية للأطراف والشهود. وكذلك بعدم الإفصاح عن البيانات إلا بموجب أمر قضائي أو قانوني. مع اتخاذ تدابير تقنية وتنظيمية لمنع تسرب البيانات أثناء تداولها إلكترونيا كما سبق الشرح.

من السرد السريع لأهمية النقاط في القوانين السابق ذكرها يمكن القول إن القوانين الأربعة تتقارب في المبادئ الأساسية لحماية البيانات الشخصية، لكنها تختلف في بعض التفاصيل التنظيمية والعقوبات حيث إن مصر والسعودية تتشددان في العقوبات وتضعان شروطاً صارمة لنقل البيانات خارج الحدود. بينما الإمارات تركز على التوافق مع المعايير الدولية وتفرض غرامات مالية كبيرة، فيما تولي المغرب أهمية لدور اللجنة الوطنية في الترخيص ومراقبة المعالجة.

كما يلاحظ أن جميع الدول تشترط موافقة صريحة وقابلة للسحب، وتمنح الأفراد حقوقاً قوية في الوصول والتصحيح والحذف وخصوصا في سياق التقاضي الإلكتروني، الذي يبرز فيه أهمية التدابير التقنية والتنظيمية لحماية البيانات أثناء تداولها رقمياً كحق أساسي للمواطنين.

النتائج

- الفجوة التشريعية: بالتحليل المقارن بين التشريعات محل البحث والمعايير الدولية المتطلبة فيما يتعلق بحماية البيانات الشخصية وجد أن هناك فجوة بينية يجب أن يتداركها المشرع مستقبلا
- عدم مواكبة التطورات التكنولوجية: التشريعات السابقة أيضا لا تواكب التطورات السريعة للتكنولوجيا المستخدمة في مجال التقاضي الالكتروني والجرائم المعلوماتية مما يضعف من الحماية القانونية للبيانات المتخذة بتلك الدول
- تأثير التقاضي الالكتروني على الحقوق الرئيسية المقررة للمواطنين: حيث إن التوسع في استخدام التقاضي الالكتروني والبيانات المقدمة له تتعارض مع بعض الحقوق الدستورية للأشخاص مثل الحق في الخصوصية وحماية البيانات.
- تفاوت في مستوى الحماية :حيث إن هناك تفاوت في مستوى الحماية القانونية للبيانات الشخصية بين القانونين المصري والسعودي في سياق التقاضي الإلكتروني.

التوصيات

- تحديث التشريعات :ضرورة تحديث وتطوير القوانين المصرية والسعودية المتعلقة بحماية البيانات الشخصية وجرائم تقنية المعلومات بما يتناسب مع التطورات التكنولوجية في مجال التقاضي الإلكتروني والمعايير الدولية.
- تعزيز آليات الحماية :يجب تطوير مستمر لآليات تقنية وإدارية وقانونية أكثر فعالية لضمان أمن وسرية البيانات الشخصية في الأنظمة الإلكترونية للمحاكم.
- تفعيل دور الجهات الرقابية :يجب تعزيز دور الهيئات والجهات الرقابية المسؤولة عن حماية البيانات الشخصية وتزويدها بالصلاحيات والموارد اللازمة لإنفاذ القوانين ومراقبة الامتثال.
- مواءمة التشريعات مع الاتفاقيات الدولية :يجب العمل على مواءمة التشريعات الوطنية مع المبادئ والمعايير الواردة في الاتفاقيات الدولية المتعلقة بحماية البيانات الشخصية والجرائم المعلوماتية.
- تطوير آليات لضمان المساءلة :يجب وضع آليات أكثر ردعا عن أي انتهاكات للبيانات الشخصية تحدث في سياق التقاضي الإلكتروني.

(ISSN: 2356 - 9492)

الخاتمة

إن التقاضي الإلكتروني يعتبر حل جذري لبطء التقاضي وكذلك للارتقاء بالسلك القضائي لتقليل تدخل العنصر البشري في مجال القضايا. ولتقليل الوقت والجهد والمال. إلا ولأن التطور التكنولوجي كما أن له وجه إيجابي إلا أن وجهه السلبي لا يمكن التغاضي عنه مثل عدم تواجد أو ضعف تواجد شبكات الانترنت في العديد من الدول، كذلك انتشار القرصنة والفيروسات. كذلك التفاوت الهائل في التقنيات بين الدول المتقدمة والنامية مما يخلخل معايير العدالة. كذلك سرقة المعلومات والبيانات الخاصة بالمتقاضين واختراقها والعبث بها وتشويه سمعة مالكيها. وفي النهاية التباطؤ والقصور في مجابهة التشريعات للتطورات المجال الرقمي. هذه سلبيات لابد من العمل على تلافيها ويمكن لتلافي تلك الأوجه السلبية ما يأتي بأن تكون هناك بنية تحتية قوية للتقاضي الالكتروني من أجهزة حديثة وشبكة أنترنت قوية وفريق تقني متخصص وتدريب للقضاة والعاملين بالقضاء الالكتروني والمحامين على كيفية عمل منظومة التقاضي عن بعض. سن تشريعات متطورة تتناسب مع التطورات الحاصلة في المجال التقني ولا يقتصر واضعوها فقط على رجال القانون، بل يشترك معهم متخصصين في مجال الأمن السيبراني.

المصادر

١. حازم شرعة، التقاضي الإلكتروني والمحاكم الإلكترونية، ط١، دار الثقافة للنشر والتوزيع، الأردن،٢٠١٠
٢. أسعد منديل، التقاضي عن بعد دراسة قانونية، مجلة الكوفة للعلوم القانونية والسياسية، عدد٢١، المجلد٧، العراق،٢٠١٤.
٣. أمير فرج يوسف، المحاكم الإلكترونية والمعلوماتية والتقاضي الإلكتروني، المكتب العربي الحديث، الإسكندرية، ط١، ٢٠١٤
٤. عبد الله المرزوقي، التقاضي الإلكتروني والكترونية التقاضي، دراسة مقارنة، مجلة الشارقة للعلوم القانونية، العدد ٢٤٤. المجلد ١٨، ص٢٠٢١
5. Nguyen, Linh, A Preliminary Survey,19th Australian Conference on Information System – "(2008).
٦. مصطفى المتولي قنديل، حماية الخصوصية المعلوماتية للمتقاضين أثناء المحاكمة عن بعد أمام المحاكم الإماراتية، مجلة جامعة العين للأعمال والقانون، الإصدار الثاني، السنة السابعة، الإمارات. ٢٠٢٢.
٧. أيمن مصطفى البقلي، حماية الخصوصية المعلوماتية لمستخدمي الإنترنت في مواجهة التجارة الإلكترونية، المجلة القانونية، كلية الحقوق، جامعة القاهرة، المجلد٩، العدد ٤، ٢٠٢١.
٨. قانون حماية البيانات الشخصية المصري رقم ١٥١ الصادر في ٢٠٢٠ المنشور بالجريدة الرسمية – العدد ٢٨ مكرر (هـ) – في ١٥ يوليه سنة ٢٠٢٠ والذي عمل به بعد ثلاثة أشهر من تاريخ نشره.
٩. أشرف جودة محمد محمود، المحاكم الإليكترونية في ضوء الواقع الإجرائي المعاصر، مجلة الشريعة والقانون، العدد ٣٥، الجزء ٣، ٢٠٢٠.
10. ES250132_PREMS 005419 GBR 2013 charte éthique CEPEJ WEB A5.pdf
١١. حاتم جعفر، التقاضي الإلكتروني والأمن السيبراني "دراسة حالة للمحاكم المصرية". بحث مقدم للمؤتمر الدولي السنوي ٢٣ الأبعاد القانونية والاقتصادية لمنظومة التقاضي في القرن الحادي والعشرين من الفترة من ٢٢/٢١ أبريل ٢٠٢٤

(ISSN: 2356 - 9492)

١٢. القانون الإماراتي رقم ٥ لسنة ٢٠١٧ في شأن استخدام تقنية الاتصال عن بعد في الإجراءات الجزائية المنشور بالجريدة الرسمية العدد ٦١٦.

١٣. قرار وزير العدل الإماراتي رقم ٢٥٩ لسنة ٢٠١٩ بشأن الدليل الإجرائي لتنظيم التقاضي باستخدام الوسائل الإلكترونية والاتصال عن بعد في الإجراءات الجزائية المنشور بالجريدة الرسمية العدد ٦٥١

١٤. قرار وزير العدل الإماراتي رقم ٢٦٠ لسنة ٢٠١٩ بشأن الدليل الإجرائي لتنظيم التقاضي باستخدام الوسائل الإلكترونية والاتصال عن بعد في الإجراءات المدنية المنشور بالجريدة الرسمية العدد ٦٥١

١٥. ظهير شريف رقم 1-07-129صادر في ٣٠ نوفمبر ٢٠٠٧ بتنفيذ القانون رقم ٠٥-٥٣ المتعلق بالتبادل الإلكتروني للمعطيات القانونية. والمنشور بالجريدة الرسمية العدد ٥٥٨٤.

١٦. ظهير شريف رقم ١.٠٧.١٣٤ صادر في ٣٠ نوفمبر ٢٠٠٧ بتنفيذ القانون رقم٠٧.٠٣ المتعلق بكيفية مراجعة أثمان كراء المحلات المعدة للسكنى، أو الاستعمال المهني، أو التجاري، أو الصناعي، أو الحرفي. والمنشور بالجريدة الرسمية العدد ٥٥٨٦

١٧. ظهير شريف رقم ١.٠٩.١٥ صادر في ١٨ فبراير ٢٠٠٩ بتنفيذ القانون رقم ٠٩.٠٨ المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي. والمنشور بالجريدة الرسمية العدد ٥٧١١

١٨. ظهير شريف رقم ١.٠٧.١٩٧ الصادر في ١١ نوفمبر ٢٠٠٣ بتنفيذ القانون الجنائي المغربي

١٩. ايمان محمد عبد الله القثامي، التقاضي عن بعد دراسة فقهية تطبيقية على النظام السعودي، مجلة علوم الشريعة والدراسات الإسلامية، العدد ٨٤، الصادر في مارس ٢٠٢١

٢٠. قانون حماية البيانات الشخصية المصري رقم ١٥١ لسنة ٢٠٢٠ المنشور بتاريخ ٢٠٢٠/٧/١٥ وتحديثاته حتى عام ٢٠٢٣

٢١. المرسوم بقانون اتحادي رقم ٤٥ لسنة ٢٠٢١ بشأن حماية البيانات الشخصية الصادر بتاريخ ٢٠٢١/٩/٢٠

٢٢. ظهير شريف رقم ٠٩.٠٨ **المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي**، الصادر في ١٨ فبراير ٢٠٠٩

٢٣. نظام حماية البيانات الشخصية الصادر بالمرسوم الملكي رقم ١٩ بتاريخ ٢٠٢١/٩/٢٤