Journal of Human and Social Sciences (JHSS) • Vol 7, Issue 11 (2023) • P: 94 - 82
https://journals.ajsrp.com/index.php/jhss
ISSN: 2522-3380 (Online) • ISSN: 2522-3380 (Print)

Personal Data Protection in the Kingdom of Saudi Arabia, EU and UK GDPR: A Comparative Study

Mr. Najim Abdullah Al-Shammari

College of Humanities & Social Sciences | King Saud University | KSA

Received: 09/07/2023

Revised: 21/07/2023

Accepted: 24/08/2023

Published: 30/11/2023

* Corresponding author: naarrak76@gmail.com

Citation: Al-Shammari, N. A. (2023). Personal Data Protection in the Kingdom of Saudi Arabia, EU and UK GDPR: A Comparative Study. *Journal of Humanities & Social Sciences, 7*(11), 82 – 94. https://doi.org/10.26389/AJSRP.M090723

Abstract: The Saudi Personal Data Protection policy is relatively new. It has been into effect on 15/09/2021. Then it has been revised on 30/03/2023. The purpose of this study is to shed light on the Saudi policy of personal data protection. By conducting a comparison between the Saudi Personal Data Protection policy with the European and British General Data Protection Regulations (GDPR), this paper aims to illustrate what are there in place in the European policies not yet in the Saudi. This will help identify the gabs in the Saudi policy and how those gabs are to be addressed. This makes the Saudi policy always proactive as it is going to be in alignment with scientific and technological progresses and advances. This paper undertook a literature review and visited policy and guidance documents by the relevant Saudi governmental agencies. Findings show that there are some points the Saudi Personal Data Protection does not cover such as Privacy by design and privacy impact assessment. In addition, since personal data protection and cybersecurity are new to the Kingdom of Saudi Arabia, most organizations perform without relevant policies and without hiring a dedicated personal data protection officer. This paper highlights these points and their vital role in compliance and risks management. This paper recommends considering Privacy in Design and Default, every organization has to create their own personal data protection policy and hire a dedicated officer for that. This paper also presents the tool of Privacy Impact Assessment to support evaluating personal data protection related matters.

Keywords: Personal Data Controller, Personal Data Processor, General Data Protection Principles, Fair Processing, Data Subject Rights, Privacy in Design and Default, General Data Protection Regulations (GDPR), Privacy Impact Assessment (PIA).

حماية البيانات الشخصية في المملكة العربية السعودية، الاتحاد الأوروبي والمملكة المتحدة البريطانية: دراسة مقارنة

أ. نجم بن عبد الله الشمري

كلية العلوم الإنسانية والاجتماعية | جامعة الملك سعود | المملكة العربية السعودية

المستخلص: يعتبر نظام حماية البيانات الشخصية في المملكة العربية السعودية حديثاً: فقد صدرت الموافقة عليه وأقر في 1443/02/09 وجرى تعديل نظام حماية البيانات الشخصية السعودي في 1444/9/5هـ برقم (م/148). والغرض من هذه الدراسة هو التعرف على سياسة حماية البيانات الشخصية السعودية وأهميتها والجهات الراعية لها والمسؤولة عنها. والتعرف أيضاً على الطريقة والأدوات التي تتبعها السياستين الأوروبية والبريطانية لضمان تطبيق القانون ومواكبة التقدم العلمي والتقني ومقارنتها بالأدوات السعودية بغية التطوير والتحديث اللازم في هذا المجال الحساس. لم تعتمد هذه الدراسة على استعراض الدراسات السابقة فقط، إنما استعانت بوثائق الجهات الحكومية الراعية لسياسة حماية البيانات الشخصية التي تشرح وتفسر القوانين ذات الصلة. تشير النتائج الى أن السياسة السعودية لم تتطرق الى موضوع Privacy in Design and Default أو خصوصية البيانات منذ المراحل الأولي لعملية تصميم قواعد البيانات والمواقع الإلكترونية وتطبيقات الأجهزة الذكية التي تعتمد في عملها على جمع البيانات الشخصية ومعالجتها وحفظها ومشاركتها مع الغير وأرشفتها. وأيضاً، نتيجة لحداثة عمر سياسة البيانات الشخصية والأمن السيبراني في المملكة العربية السعودية، افتقار أغلب المنظمات الحكومية وغيرها إلى سياسة لحماية البيانات الشخصية وعدم وجود مختص أو مسؤول عن سياسة حماية البيانات الشخصية. وأوصت هذه الدراسة المشرع في المملكة العربية السعودية على إدراج هذا الإجراء Privacy in Design and Default وجعله من الأولويات حيث أنه يسلط الضوء على كيفية ومستوى حماية وصيانة البيانات الشخصية وحث جميع المنظمات الى إنشاء سياسة لحماية البيانات الشخصية وتوظيف من لدية الكفاءة لمتابعة الأعمال والقيام بالتحديثات الازمة. ولكي نصل الى المستوى المطلوب، قدمت هذه الورقة أداة تقييم الأثر على الخصوصية أو ما يسمى Privacy Impact Assessment وبعض الإجراءات الإدارية المعينة على تنفيذ القانون بالشكل الصحيح.

الكلمات المفتاحية: البيانات الشخصية، جهة التحكم، الجهة المعالجة، المبادئ العامة، المعالجة العادلة، حقوق أصحاب البيانات الشخصية، الخصوصية منذ التصميم، قانون حماية البيانات الشخصية الأوروبي، تقييم المخاطر

1- المقدمة:

صدر الأمر السامي رقم م/19 بتاريخ 1443/02/09 بالموافقة على نظام حماية البيانات الشخصية ملزماً جهات التحكم والجهات المعالجة للبيانات الشخصية في القطاعين العام والخاص والأفراد بإمتثال وتطبيق ما ورد من بنود في نص النظام. وتم تعيين مركز المعلومات الوطني كجهة مختصة طبقا للأمر السامي. والمقصود بجهة التحكم هي الجهات التي تجمع البيانات الشخصية وتحدد الغرض منها وقد تكون جهة التحكم فرداً (سياسات حوكمة البيانات الوطنية، 2021).

وجرى تعديل نظام حماية البيانات الشخصية السعودي في 1444/9/5هـ برقم (م/148). وقد أولى النظام السعودي لحماية البيانات الشخصية اهتماماً كبيراً ببيانات الأطفال الشخصية ومن في حكمهم وإفرادهم بسياسة خاصة تحت مسمى سياسة حماية البيانات الشخصية للأطفال ومن في حكمهم لتكون جزءاً من سياسات حوكمة البيانات الوطنية. وبحثاً عن الكمال وسد الثغرات ما أمكن، تقارن هذه الورقة سياسة حماية البيانات الشخصية في المملكة العربية السعودية بالسياسات والتشريعات الأوروبية والبريطانية المماثلة. وسبب اختيار التشريعات اللأوروبية والبريطانية يرجع الى قوة وصرامة نظام وسياسة حماية البيانات الشخصية في تلك التشريعات تحت مسمى GDPR. وسيرد ذكر EU GDPR وUK GDPR عدة مرات في هذه الورقة. وGDPR اختصاراً ل General Data Protection Regulations

يعيش العالم ثورة في التقنية والإتصالات حيث تتم معالجة البيانات الشخصية بشكل كبير جداً في كل لحظة الأمر الذي يحتم ضرورة وجود قانون صارم لحماية الأشخاص والممتلكات. فلا يزال المواطن والمقيم على أرض المملكة العربية السعودية عرضة للإبتزاز والإحتيال الإلكتروني مع كل أسف والسؤال المهم الذي لم يجد إجابة هو كيف حصل المحتالون على البيانات الشخصية لضحاياهم من مواطنين ومقيمين؟ فأين يكمن الخلل؟

تهدف هذه الورقة الى الوقوف على مكامن الخلل عن طريق مقارنة سياسة حماية البيانات الشخصية السعودية بالقوانين المماثلة في الإتحاد الأوروبي والمملكة المتحدة تتكشف نقاط الضعف إن وجدت وهذا يتيح فرصة للمشرع في المملكة العربية السعودية بمراجعة السياسة وتحديثها بما يتماشى والقوانين الدولية ذات الصلة لتكون دائما استباقية في التعامل مع الأحداث وفعالة في كشف الحوادث والخروقات قبل حدوثها. فمن المفيد أن نعلم الفروقات وكيف استطاعت التشريعات في البلدان المتقدمة من فرض نفسها على القطاعين العام والخاص بحيث أصبح الجميع يبحث عن سبل الإمتثال لتلك القوانين والسياسات وتجنب المخالفات. ومن فوائد هذه الدراسة الإستفادة مما توصل إلية المجتمع المقدم علمياً كبريطانيا حتى هذه اللحظة من مواكبة القانون للعلم والتقنية. ومن الفوائد أيضاً، جعل تلك القوانين مألوفةً لدى المتخصصين والمسؤولين عن حماية البيانات الشخصية في المملكة العربية السعودية.

إن أهمية هذه الدراسة نابعة من أهمية محتواها حيث أنها تناولت سياسات حماية البيانات الشحصية التي تهدف لحفظ البشر من خلال حفظ بياناتهم الشخصية ومشاركتها مع الغير بطريقة عادلة ومنصفة مُنطلقةً من دوافع شرعية وقانونية من دون تمييز. وتأتي هذه التشريعات لتُوازن بين الحاجة إلى معالجة البيانات الشخصية من جهة، وحمايتها من جهة أخرى (هوفمان وآخرون، 2017). وقد وافق علي (2021) هوفمان وآخرون (2017) في أن تشريعات وسياسات حماية البيانات الشخصية تُنظم وتُوازن الطلب على البيانات الشخصية وحمايتها. ويجسد قانون حماية البيانات الشخصية حرص القيادة السعودية وفقها الله وسدد خطاها على أمن وسلامة المواطنين والمقيمين على أرض المملكة بإختلاف جنسياتهم حيث إنشاء القوانين والتشريعات اللآزمة والضرورية لحماية بياناتهم الشخصية في زمن تُتداول فيه البيانات بشكل كبير جداً وسريع. فكلما زادت العمليات والمعالجات للبيانات الشخصية ارتفعت نسبة الخطورة. فشكلت هذه السياسات، سياسات حوكمة البيانات الوطنية (2021) ومن بينها نظام حماية البيانات الشخصية، استجابة المملكة العربية السعودية للأوضاع الحالية ومحاولةً لدرء المخاطر الناتجة عن التصرفات الغير سليمة فيما يتعلق بأمن وحماية البيانات الشخصية.

وسيدرك أصحاب البيانات الشخصية وجهات التحكم والجهات المعالجة أهمية وفوائد هذا النظام فور تطبيقة إن لم تكن معلومة سلفاُ. فأعداد ضحايا عمليات انتحال الشخصية والسرقات الإلكترونية والإبتزاز في البيئات الرقمية آخذ بالإرتفاع. ولا بد من رقيب يراقب كيفية معالجة البيانات الشخصية في قواعد البيانات الخاصة بالمؤسسات ويراقب آلية مشاركة البيانات مع الجهات والأشخاص الآخرين (الشيتي، 2014). وليس الغرض من عملية المراقبة خلق عقبات أمام إنجاز المعاملات اليومية على البيانات الشخصية. إنما الهدف هو الحد من التجاوزات وترسيخ الممارسات الإيجابية والتخلص من الممارسات السلبية بما فيها تلك التي تدور في أروقة وسائل التواصل الإجتماعي (أحمد، 2017).

فالفائدة الأهم هي تعزيز حماية الأشخاص وممتلكاهم. إلا أن فوائد نظام حماية البيانات الشخصية لا يقف عند الأفراد بل يتعدى ليشمل المؤسسات، حيث أن نظام حماية البيانات الشخصية يساعد المؤسسات على الحفاظ على طاقاتهم البشرية من الضياع

ومن خسارتهم لصالح منافسيهم. وأيضا، قد يكون تسرب البيانات الشخصية سبباً في تهديد كيان المؤسسة خصوصاً إذا كان أو كانت الضحية من أصحاب صناعة القرار والنفوذ. كان هذا على الصعيد الوطني الداخلي.

أما على الصعيد الدولي، فأهمية قانون حماية البيانات الشخصية لا تقل بحال من الأحوال عن أهميته وفائدته في الداخل السعودي. فمن الفوائد ماهو سياسي ومنها الإقتصادي والثقافي والرياضي. فسياسياً، هذا النظام، عند تطبيقه، يعزز ثقة المجتمع الدولي بالمملكة العربية السعودية. لاشك أن للمملكة مكانة كبيرة ودور ريادي في الإقليم وعلى مستوى العالم أيضا. ولعل عضويتها في قمة العشرين خير شاهد على ذلك. وقمة العشرين هي مجموعة مكونة من عشرين دولة من الدول الأقوى اقتصادياً في العالم (g20.org) . فالتكتلات السياسية والتحالفات لها قوانينها الخاصة بها، على سبيل المثال، دول الإتحاد الأوروبي تحكم قانونا صارماً وشاملاً لحماية البيانات الشخصية يطلق عليه اسم: "التنظيمات العامة لحماية البيانات الشخصية GDPR". وبطبيعة الحال، فإن الدول الأعضاء في الإتحاد الأوروبي داخلة في نطاق القانون أو التشريع أما الدول الخارجة عن جغرافية الإتحاد الأوروبي تكون في ضمن النطاق ولا بد أن تمتثل بما جاء فيه من بنود إذا كان بعض مواطني الإتحاد الأوروبي يعملون ويقيمون في دول غيرها كالمملكة العربية السعودية اليوم. فالمملكة داخلة في نطاق القانون الأوروبي لحماية البيانات الشخصية نتيجة لتوافد مواطني الإتحاد للعمل والعيش في المملكة (الفقرة 104 من EU GDPR). وهذا يستوجب أن يكون لدى المملكة قانوناً سعودياً مستقلاً مماثلاً ومتماشياً مع الأعراف والقوانين الدولية. وهذا هو الهدف من هذه الدراسة؛ المقارنة وكشف الإختلاف.

بعد الحديث عن الأهمية السياسية لقانون حماية البيانات الشخصية، يأتي الحديث عن الفوائد الإقتصادية. لا شك أن هذا القانون، أي قانون حماية البيانات الشخصية، يساعد في زيادة فرص الإستثمار الأجنبي في المملكة ومن شأنه أن يحول المملكة إلى بيئة جاذبة للإستثمارات الأجنبية. لاسيما إن علمنا أن هذا القانون أصبح من البديهيات وجزء من الثقافة الغربية والمجتمع الدولي. وأفاد هوفمان وآخرون (2017) أن القانون يعزز الثقة. وهذا أيضا ما ذهب إليه الباحثون الثلاثة وليام، حسنداوست، وزهانق (2020) في دراستهم التي تناولوا فيها موضوع ثقة المستهلك في سياق القانون الأوروبي لحماية البيانات الشخصية GDPR وخلصوا إلى أن حماية البيانات الشخصية تعزز وتقوي ثقة المستهلك بالمنشأة نتيجة لأسباب عدة من ضمنها الشفافية وحقوق أصحاب البيانات التي شدد القانون بحمايتها (زهانق وآخرون، 2020). وفي دراسةٍ له، اعتبر الشمري (2019) قانون حماية البيانات الشخصية من العوامل المساهمة على تعزيز ثقة المستخدم في المواقع الإلكترونية. فحماية البيانات الشخصية عامل تشجيعي ومحفز للمستثمرين ومصدر ثقة الأجانب للإستثمار في السوق السعودي حيث التنوع والإتساع. أضف إلى ذلك، ستكون الشركات الدولية الكبرى ذات العلاقات التعاقدية مع المملكة مطمئنة بإرسال من ترى من الخبراء والمهندسين والمسوقين الى المملكة لتبادل المنافع وفي هذا إسهام لتحقيق رؤية المملكة 2030 (رؤية المملكة 2030). كما أنه يدعم الأجندة السعودية المتمثلة في نقل التقنية من خلال استقطاب الكفاءات الأجنبية للعمل والتدريب. وهذه الفئة المستهدفة ليس بمقدورهم أن يباشروا أعمالهم في المملكة كما هو مخطط له من غير ضمانات على سلامتهم وحماية بياناتهم وممتلكاتهم. وتتقابل المنفعة الإقتصادية وتتحقق أيضا من خلال المجال الثقافي والرياضي على حدٍ سواء، فستكون المملكة العربية السعودية بيئةً جاذبةً للسياح الأجانب والمحترفين الرياضيين الذين يرغبون في الإنضمام الى صفوف الأندية السعودية نتيجةً لتفعيل نظام حماية البيانات الشخصية في أمن وسلامة القادمين للمملكة العربية السعودية وبالتالي سيكون له أثراً إيجابياً على الإقتصاد الوطني (رؤية المملكة 2030).

بناءً على ما سبق ذكره، أصبحت أهمية نظام حماية البيانات الشخصية واضحة وجلية وتحقيقاً للمصلحة العامة، تم إقرار قانون حماية البيانات السعودي كما ذكر آنفا. وتهدف هذه الورقة لتعزيز سبل الإستفادة من هذا القانون ما أمكن ولفت أنظار أصحاب القرار الى ما يمكن إدراجه والعمل به لتحقيق الهدف المنشود. ويكمن التحدي في تطبيق هذا القانون كونه تشريعا جديداً على أمتنا العربية بشكل عام وعلى المملكة العربية السعودية بشكل خاص وهذا يتطلب جهدا كبيراً من الجهات ذات الإختصاص بالتعريف عن هذا التشريع ومتابعة الأعمال. ومن أهداف هذه الورقة المساعدة على التعرف على الآليات المتبعة في كل من الإتحاد الأوروبي والمملكة المتحدة لتنفيذ وتطبيق القانون.

ولأغراض هذه الورقة، تكون الأسئلة البحثية كالآتي: مالمقصود بالبيانات الشخصية؟ هل سياسة حماية البيانات الشخصية في المملكة العربية السعودية متطابقة ومتماشية مع القوانين الدولية من حيث القانون والآليات المتبعة؟ ومالمَواطن التي تحتاج الى مزيد من التركيز في السياسة السعودية لحماية البيانات الشخصية؟ وللإجابة على هذه الأسئلة، قُسمت هذه الدراسة الى قسمين رئيسيين هما: البعد القانوني والبعد الإجرائي. ففي البعد القانوني أوردت هذه الدراسة بعض التعريفات وفقاً للقوانين ذت الصلة. وأيضاً تم مقارنة المبادئ العامة لحماية البيانات الشخصية، الجمع العادل للبيانات الشخصية، حقوق أصحاب البيانات الشخصية ومشاركة البيانات الشخصية في السياسة السعودية والإتحاد الأوروبي والمملكة المتحدة البريطانية بغية التطوير والتقدم. أما في البعد الإجرائي، تقدم هذه الورقة أهم الآليات المتبعة لضمان تنفيذ القانون والإمتثال لما جاء به من بنود وتحقيق الأهداف المنشودة من إنشائه وإقرارة.

2- البعد القانوني

2-1 التعريفات والنطاق

ورد تعريف البيانات الشخصية في سياسات حوكمة البيانات الوطنية على أنها، "كل بيان - مهما كان مصدره أو شكله - من شأنه أن يؤدي إلى معرفة الفرد على وجه التحديد، أو يجعله قابلاً للتعرف عليه بصفة مباشرة أو غير مباشرة عند دمج هذا البيان مع بيانات أخرى، ويشمل ذلك -على سبيل المثال لا الحصر-الاسم، أرقام الهويات الشخصية، والعناوين، وأرقام التواصل، وأرقام الحسابات البنكية، والبطاقات الإئتمانية، وصور المستخدم الثابتة والمتحركة، وغير ذلك من البيانات ذات الطابع الشخصي".

وأيضاً، جاء في قائمة التعاريف من سياسات حوكمة البيانات الوطنية (2021) أن الجهات المعالجة يقصد بها تلك الجهات، سواءً حكومية أو غير ذلك، التي تعالج البيانات الشخصية وقد تكون في بعض الأحيان تعالج البيانات الشخصية بالنيابة عن جهة التحكم.

وطبقاً لسياسات حوكمة البيانات الوطنية، تُعرف معالجة البيانات الشخصية على أنها جميع العمليات التي تتم على وتمر بها البيانات الشخصية من جمع، وتحليل، ومشاركة مع الغير، وتخزين، وصولاً بالإتلاف. ومن خلال مقارنة التشريعات قيد الدراسة، يتضح أن هناك اتفاق كبير جداً بالتعريفات المتعلقة بسياسة حماية البيانات الشخصية فقد ورد تعريفاً مطابقاً للبيانات الشخصية وكيفية معالجتها في كل من القانون البريطاني والأوروبي وفقاً لما أورده مكتب مفوض المعلومات البريطاني What is personal information: a guide | ICO والفقرة الرابعة من القانون الأوروبي المتعلقة بالتعريفات Art. 4 GDPR Definitions

وهذا لا يقتصر على البيانات الشخصية التي تتم معالجتها إلكترونياً أو آلياً فقط، بل يشمل أيضاً تلك المحفوظة يدوياً والمُؤرشفة (سياسات حوكمة البيانات الوطنية، 2021). وهذا له ما يقابله في القانونين الأوروبي والبريطاني. ففي الفقرة الرابعة من قانون EU GDPR ورد تعريف لنظام الأرشفة الذي ينطبق علية قانون حماية البيانات الشخصية وداخل في نطاقة. فالإستنتاج هنا أن البيانات الشخصية ليست مقتصرة على تلك البيانات التي يتم تداولها في العالم الإفتراضي فقط وإنما تشمل المؤرشف منها وما يتناول يداً بيد.

أما أصحاب البيانات الشخصية فهم الأشخصاص الطبيعيين الذين تتعلق بهم البيانات الشخصية والذين من الممكن التعرف عليهم من خلالها ويشمل هذا كل من يمثل أصحاب البيانات الشخصية أو من له الولاية عليهم طبقا لما أوردته سياسات حوكمة البيانات الشخصية. ومن هذا التعريف نستنتج أن سياسات حماية البيانات الشخصية لا تشمل وليس من نطاقها الأشخاص المتوفين وهذا مادلت علية كلمة "أشخاص طبيعيين". وفي هذا اتفاق مع القانونين البريطاني والأوروبي عندما عرفوا أصحاب البيانات الشخصية ووصفوهم بأنهم أشخاص على قيد الحياة 'Living Individual' (ICO & EU GDPR Art. 4 Definitions) .

2-2 المبادئ العامة لحماية البيانات الشخصية:

سطر مكتب إدارة البيانات الوطنية(sdaia.gov.sa) المبادئ العامة لحماية البيانات الشخصية موضحة بالشكل أدناة. أما مبادئ حماية البيانات الشخصية في السياسة البريطانية فمأخوذة من مكتب المعلومات البريطاني Information Commissioner's Office (ICO). اما المبادئ العامة لحماية البيانات الشخصية في السياسة الأوروبية فمأخوذة من GDPR Archives - GDPR.eu

المبدأ	السياسة السعودية	السياسة البريطانية	السياسة الأوروبية
إنشاء سياسة لحماية البيانات الشخصية	✓	✓	✓
الشفافية في جمع البيانات ومعالجتها	✓	✓	✓
موافقة أصحاب البيانات الشخصية ضرورة للمعالجة	✓	✓	✓
الإقتصار على الحد الأدنى من البيانات الشخصية للغرض الواحد	✓	✓	✓
يجب على المنظمات حفظ وصيانة البيانات الشخصية وعدم السماح بالوصول اليها الا للأشخاص المخولين	✓	✓	✓
يجب منه الأطراف الخارجية من الوصول الى البيانات الشخصية الا في أضيق نطاق وبعد موافقة أصحابها	✓	✓	✓
يجب أن تكون البيانات محدثة وذات جودة عالية لتخدم الغرض الذي من أجله جمعت	✓	✓	✓
توفير الحماية للبيانات الشخصية من التسرب والضياع والسرقة	✓	✓	✓

المبدأ	السياسة السعودية	السياسة البريطانية	السياسة الأوروبية
المراقبة والإمتثال للقوانين والسياسات ومراعات التحديثات	✓	✓	✓
الخصوصية بدأً من التصميمPrivacy by Design	✗	✓	✓
حماية البيانات يجب أن يكون من التصميم وبشكل بديهي Privacy by Design and by Default	✗	✓	✓

يتضح لنا مما سبق التطابق الكبير بالمبادئ العامة لحماية البيانات الشخصية إلا أن السياسة السعودية لم تتطرق لموضوع الخصوصية بدأً من التصميم Privacy by Design وهذا موضوع مهم حيث تبدأ عملية خصوصية البيانات من عملية تصميم السياسات وقواعد البيانات ومستودعاتها وتصميم النماذج المتعلقة بطلبات الوصول الى البيانات الشخصية. وهذا يعزز مفهوم الأستخدام العادل للبيانات. ونظراً لأهمية هذا المبدأ، أفردت له هذه الورقة قسماً خاصاً ليتم التعرف عليه بالتفصيل.

وصفت جميع تشريعات وسياسات حماية البيانات الشخصية قيد الدراسة الإستخدام الصحيح واللآئق للمعلومات الشخصية على أنه الأستخدام العادل. أي أنه ذلك الإستخدام الذي لا يخالطه جور ولا ظلم ولا إساءة للأفراد من خلال سوء استخدام بياناتهم الشخصية (سياسات حوكمة البيانات الوطنية، 2021 وEU GDPR & UK GDPR). وقد استخدم ذات الوصف فلوريدي عندما تكلم عن أخلاقيات المعلومات ووصف المعلومات بأنها مصادر يجب أن تعامل بعدل (فلوريدي، 2013). وسوف تَرِد في هذه الدراسة عبارة "الإستخدام العادل" أكثر من مرة نظراً لإجماع السياسات قيد الدراسة عليها تأكيداً لأهميتها.

ولترسيخ الأستخدام العادل للبيانات الشخصية، لابد أن يكون لكل مؤسسة أو هيئة حكومية كانت أو غير ذلك سياستها الخاصة لحماية البيانات الشخصية. إلا أن جميع السياسات يجب أن تتوافق مع السياسة الأم، وهي التي تتحدث عنها هذه الورقة. فمن غير المنطقي أن تكون مؤسسة سعودية تطبق سياسة تتعارض مع سياسة المملكة. على سبيل المثال، بإمكان جامعة الملك سعود إنشاء سياسة بيانات شخصية خاصة بها تهدف الى حماية البيانات الشخصية لجميع منسوبي الجامعة والمستفيدين من الخدمات الطبية لأن الجامعة هي أدرى من غيرها بتصريف وأولويات الأعمال الأكاديمية، والطبية والإدارية التي تتطلب معالجةً للبيانات الشخصية بشكل يومي.

وقد حثت سياسات حوكمة البيانات الوطنية المؤسسات على إنشاء سياسة لحماية البيانات الشخصية كل مؤسسة بما يخدم مصالحها. ويعتبر هذا الإجراء من أسباب الإمتثال الناجح (سياسات حوكمة البيانات الوطنية 2021). وزيادة في التأكيد، وجب التنويه الى أنه عند تصميم سياسة حماية البيانات الشخصية يجب مراعاة أهداف المنظمة (جهة تحكم) وحاجتها لمعالجة البيانات الشخصية من جهة والحماية من جهة أخرى (هوفمان وآخرون، 2017). ولقد أولت القوانين الدولية موضوع التصميم أهمية بالغة حيث أُفرد بفقرةً مستقلة في القانون البريطاني (UK GDPR) والقانون الأوروبي تحت مسمى، "حماية البيانات حسب التصميم وبشكل بديهي"(EU GDPR, Art.25). هذا يعني أن وضع التدابير التقنية والتنظيمية لتنفيذ مبادئ حماية البيانات الشخصية متطلب قانوني. والغرض من هذا المتطلب القانوني هو أن يدمج نظام حماية البيانات الشخصية في ممارسات الأشخاص في المنظمات بدأً من عملية التصميم وحتى مرحلة التنفيذ في العمليات اليومية (UK GDPR). كانت هذه الوصية الأولى والتي لا ينبغي على أي مؤسسة، هيئة، أو منظمة في المملكة تجاهلها. إن إنشاء وتصميم سياسة حماية بيانات شخصية مستقلة وخاصة بكل كيان أو تنظيم يخدم مصالحهم ونشاطاتهم التجارية والإدارية من عوامل النجاح. لكن، يجب أن تكون السياسات متماشية مع السياسة العامة للمملكة. ويجب أن يعاد تقييم جميع السياسات وتراجع من حين لآخر لغرض ضمان مواكبتها التقدم العلمي والتقني (الشيتي، 2014).

إضافة إلى ما تم ذكره، يجب أن تقوم جهة التحكم بإنشاء وحدة لحوكمة البيانات يكون من مهامها ضمان إمتثال الأنظمة والقوانين واتباع السياسات والتماشي مع التحديثات الطارئة من خلال فريق عمل مدرب بشكل جيد ومتخصص في سياسات البيانات الشخصية (سياسات البيانات، 2021). من الضروري إنشاء فريق حوكمة السياسات أو على أقل الأحوال موظف مختص (سياسات حوكمة البيانات، 2021) يكون من مهامه التواصل المستمر مع جهة الإختصاص، مركز المعلومات الوطني، لمواكبة وضبط التحديثات الطارئة على النظام أولاً بأول. ومن المهام أيضاً، متابعة أداء المنظمة ومنسوبيها وإرشادهم وتوعيتهم ويكون طرفاً في مراجعة العقود مع المزودين والممولين (جهات معالجة) كشركات تقنية المعلومات، التأمين، الأندية الرياضية، شركات السفر، وتأجير السيارات ممن يعالجون البيانات الشخصية بشكل يومي لتوفير خدمات للموظفين كأجهزة الكترونية وشبكات اتصال، والتأمين الصحي وغير ذلك. لكن قبل اختيار الممول، وقبل التعاقد مع أي جهة لتكون جهة معالجة، يجب أن تتساءل المنظمة (جهة التحكم) إذا كان موضوع خصوصية المعلومات وحماية البيانات الشخصية من اهتمام الشركات التي رفعت الطلبات لتكون جهات معالجة. وقد اتفقت السياستين الأوروبية والبريطانية مع السياسة السعودية في هذه النقطة وألزمت جميع المنظمات بتعيين الشخص المناسب لمراقبة أداء المنظمة وامتثالها

الأنظمة والقوانين المتعلقة بحماية البيانات الشخصية لضمان تحقيق الإستخدام العادل للبيانات الشخصية وموازنة الحاجة لمعاجة البيانات وحمايتها (UK GDPR & EU GDPR).

كيف يتحقق التوازن بين الحاجة لمعالجة البيانات لأغراض شرعية وحمايتها؟ يتحقق التوازن إذا تحققت المعالجة العادلة للبيانات الشخصية (غالب، 2019). وكيف تكون المعالجة عادلة؟ تكون المعالجة عادلة إذا توفرت فيها: أولاً، جمع البيانات بعدل أي لا يُجمع أكثر من الحاجة. ثانياً، حقوق أصحاب البيانات الشخصية، أي مالذي لهم ومالذي عليهم. ثالثاً، الإفصاح ومشاركة البيانات العادل أي لاترسل البيانات الشخصية لأي طرف كان بدون موافقة صاحب البيانات الشخصية أو موافقة أولياء الأمور إن كان أصحاب البيانات الشخصية أطفالاً أو من في حكمهم (سياسات حوكمة البيانات الوطنية، 2021). رابعاً، عند الرغبة في تطوير وتحديث قواعد البيانات التي تعالج البيانات الشخصية أو عند الحاجة الى استبدالها، لابد أن تراجع الآثار المترتبة على خصوصية البيانات الشخصية وهذا التمرين أو التقييم يسمى في قانون GDPR بـ(PIA) Privacy Impact Assessment. خامساً، لابد أن تحتوي سياسة حماية البيانات الشخصية على تعليمات بشأن التعامل مع الحوادث وكيفية إدارتها Incident Management. وستناقش هذه الورقة كل من هذه الشروط فيما يلي مع ذكر أوجه التوافق والإختلاف بين السياسة السعودية والسياسات الأوروبية.

2-3 الجمع العادل للمعلومات:

في السابق وتحديداً قبل ثورة الإتصالات، كان الفرد يذهب بنفسه شخصياً ليسلّم ملفه الشخصي لمنظمة ما بغية الحصول على عمل، فلم تكن قنوات جمع المعلومات متعددة كما هي في وقتنا الحاضر بل كانت محدودة وكذلك كانت طرق معالجتها، أيضا محدودة. أما اليوم، فالأغلب أن لكل فردٍ من أفراد المجتمع أكثر من حساب في العالم الإفتراضي موزعةٌ على وسائل التواصل الإجتماعي والمواقع المهنية ومواقع السيرة الذاتية. وقد تكون معلومات الفرد الشخصية في موقع من المواقع مكررة ومتطابقة لمحتوى موقع آخر، وقد تكون مكملة لبعضها إذا جُمعت، أو قد تكون متناقضة نظراً للعامل الزمني وتحديث البيانات. وإذا أراد الفرد أو الشخص التقدم للمنافسة على وظيفة في أحد الجهات العامة أو الخاصة، قد يرفع طلب التقديم عبر موقع المنظمة الإلكتروني، وقد يقصد حساب المنظمة في وسائل التواصل الإجتماعي ويقوم بإرسال معلوماته، وفي الوقت نفسه، يرسل معلوماته الشخصية عبر البريد الإلكتروني لأحد العاملين في المنظمة. في هذا الموقف، شخص واحد استخدم أكثر من منصة أو أسلوب لمشاركة بياناته الخاصة لنفس الغرض (غرض التقدم للمنافسة على وظيفة). وهذا من خصائص البيانات الضخمة، حيث توافد البيانات بحجم كبير، بسرعة كبيرة وقيمة عالية (ساقي وجاين، 2018). ليس غريباً أن نسمع أن عدد المتقدمين على فرصة عمل بمنظمة ما، تجاوز مئة الف. فكما ورد سابقاً قد تكون البيانات مكررة. والجمع العادل في هذا الموقف أن لا يُقصد العالم الإفتراضي لجمع المزيد من بيانات الأشخاص من غير علمهم حتى وإن كانوا من الراغبين لشغل وظيفة ما في منظمة ما. فإذا كانت الحاجة ملحة لمزيد من المعلومات، ينبغي أن تكون الحاجة مبررة وشرعية ومن ثم التواصل مع أصحاب البيانات الشخصية لطلب المزيد من بياناتهم.

وصف القانون الأوروبي GDPR الجمع العادل للمعلومات بأنه العملية التي يكون فيها الجمع واضح المعالم. بمعنى، أن يكون نوع البيانات الشخصية وحجمها معروفة ولابد أن يكون ما طُلب أو جُمع من بيانات متوازن مع الغرض الذي جُمعت من أجلة. وهذا الغرض يجب أن يكون محدداً، واضحاً، شرعي وقانوني. مثلاً، ليس من المنطق أن تطلب مكتبة أكاديمية بيانات شخصية حساسة لتمنح الطلاب تصاريح دخول. فتصريح الدخول غرض ممكن أن يتحقق بأقل قدر من المعلومات الشخصية ليست الحساسة مثل الرقم الطلابي الجامعي. فالإكتفاء بالحد الأدنى من البيانات الشخصية فيه إمتثال للسياسة السعودية لحماية البيانات الشخصية (سياسات حوكمة البيانات الشخصية، 2021). فمبدأ الإستخدام العادل أو المعالجة العادلة محل إتفاق بين السياسات قيد الدراسة.

2-4 حقوق أصحاب البيانات الشخصية:

ما وضعت سياسات حماية البيانات الشخصية إلا لحفظ حقوق أصحابها. وأول حق من حقوق صاحب البيانات الشخصية هو معرفته أو معرفتها بالأسباب التي دعت إلى جمع البيانات والأغراض التي ستعالج البيانات من أجلها. ومعرفة الجهات التي يتم مشاركة البيانات معها. فلابد أن يبلغ أصحاب البيانات بالجهات التي تستفسر عن بياناتهم وهذا ليس على الإطلاق بل فية تفصيل سيأتي الحديث عنه في فقرة المشاركة والإفصاح عن البيانات. ثانيا، لابد من الحصول على موافقة صاحب البيانات الشخصية سواءً كانت موافقة صريحةً أو ضمنية (سياسات حوكمة البيانات الوطنية، 2012). وهنا أيضا محل إتفاق بين السياسات حيث أن السياستين الأوروبية والبريطانية اشترطتا موافقة صاحب البيانات الشخصية قبل معالجتها (UK & EU GDPR). مثال، لو أن شركة ما، تواصلت مع أحد الأشخاص بغرض التوظيف، وجُمعت بياناته أو بياناتها لذلك الغرض، ثم صدر العقد الوظيفي موضحاً تاريخ بداية الخدمة، والمسمى الوظيفي وغيرذلك من التفاصيل. عندما يقبل صاحب أو صاحبة البيانات الشخصية ويوقع أو توقع على العقد، يعتبر هذا

موافقة صريحة يخول الشركة بحفظ البيانات الشخصية في منظومتها الكترونياً ويدوياً، وفيه أيضاً موافقةٌ ضمنية أو غير مباشرة في أن تشارك الشركة البيانات الشخصية مع شركات التأمين، مثلاً، لتوفير الغطاء الطبي لصاحب أو صاحبة البيانات الشخصية. لكن يجب أن يحتوي العقد فقرة عن حماية البيانات الشخصية تنص على أن للشركة الحق أن تشارك البيانات الشخصية مع الجهات التي تدعم وتساند صاحب أو صاحبة البيانات الشخصية في التوظيف وأثناء أدائهم المهام التي أوكلت لهم.

الحق الثالث من حقوق أصحاب البيانات الشخصية هو أن يكون تحديث البيانات متاحاً في كل الأوقات (سياسات حوكمة البيانات الشخصية، 2021). وهذا الحق مضمون في السياستين الأوروبية والبريطانية (UK & EU GDPR). الحق الرابع يعطي الحق لأصحاب البيانات الشخصية في مسح وإلغاء بياناتهم الشخصية (EU GDPR Art.17) و(سياسات حوكمة البيانات الشخصية، 2021). إضافةً إلى ذلك، يحق لأصحاب البيانات الشخصية تقديم الشكاوى والإعتراضات على الطريقة التي تمارس وتعالج فيها بياناتهم الشخصية عبر الوسائل القانونية المتاحة (سياسات حوكمة البيانات الشخصية، 2021). وضمنت جميع السياسات قيد الدراسة هذا الحق لصاحب البيانات الشخصية.

شددت جميع السياسات قيد الدراسة على حق الوصول للبيانات الشخصية، وهذا الحق يضمن لصاحب البيانات الشخصية طلب نسخة من جميع ما تملك المنظمة من البيانات الشخصية التي بحوزة المنظمة المتعلقة بذات الشخص أو صاحب البيانات. كوبر ولينسدورف (2022) يرى ان المقصود بهذا الحق هو الحصول على نسخة من جميع بياناتهم الشخصية التي تملكها المنظمة. وهنا يأتي دور مسؤول حماية البيانات الشخصية في تقييم الطلب ودراسته ومراجعة الملف الشخصي والتأكد من عدم الإفصاح عن معلومات شخصية لأشخاص آخرين وردت بياناتهم في الملف الشخصي المطلوب. في هذه الحالة، يجب تقديم ما هو متعلق بالشخص ذاته دون غيره.

حق التصحيح؛ أي لصاحب البيانات الشخصية الحق بطلب تصحيح بياناته عندما يكتشف أن البيانات التي تحتفظ بها المنظمة عنه غير صحيحة أو جزءا منها غير دقيق ويجب على المنظمة أن ترد خلال شهر من تاريخ رفع الطلب (UK GDPR Art.16)، الحق في تقييد أو إيقاف المعالجة ويجب على المنظمة أن ترد خلال شهر من تاريخ رفع الطلب (UK GDPR Art.18)، الحق في نقل البيانات من بيئة تقنية إلى أخر (UK ICO.com) ، الحق في الإعتراض أي يحق لصاحب البيانات الشخصية طلب إيقاف معالجة بياناته أو بياناتها الشخصية للأغراض التجارية المباشرة (UK ICO.com). اتفقت جميع السياسات قيد الدراسة على أن لصاحب البيانات الشخصية بعض الحقوق التي يجب على صاحب العمل، جهة التحكم أو جهات العالجة التقيد.

5-2 الإفصاح ومشاركة البيانات:

من دون الإفصاح ومشاركة البيانات تتوقف الحياة حيث انعدام دوران البيانات بين الأطراف ذات العلاقة لتحقيق الهدف الذي جُمعت من أجلة. لكن، هذا ليس على إطلاقه. بل له شروط واستثناءات. من الشروط ما هو مرتبط بحق من حقوق أصحاب البيانات الشخصية وهي إبلاغ وموافقة أصحاب البيانات خصوصاً إذا كانت الجهة التي تطلب البيانات جهة خارجية أي خارج المنظمة وهذا محل اتفاق بين السياسات الثلاث. سياسات حوكمة البيانات الوطنية (2021) أفادت بأن آلية الطلب تبدأ بإكمال نموذج مشاركة البيانات الذي يوضح هوية الجهه، الغرض والبيانات المطلوبة. ومن واقع خبرة، هنا يأتي دور مسؤول حماية البيانات الشخصية بتقييم الطلب والبت في القرار الإداري إما بالإفصاح والمشاركة أو المنع. وإذا كانت الجهات الخارجية، خارج المنظمة، حكومية وتطلب البيانات الشخصية لدواعي أمنيه أو صحية تصب في المصلحة العامة، فلا يجب إخبار أصحاب البيانات بهذا النوع من الطلب والمعالجة، والمنظمة بهذا لاتزال ممتثلة للأنظمة والقوانين (سياسات حوكمة البيانات الوطنية،2021). والسبب بعدم إبلاغ أصحاب البيانات الشخصية بهذا النوع من الطلب هو مخافة أن تفشل العملية الأمنية أو الصحية إذا علم أصحاب البيانات الشخصية بهذا الإجراء على بياناتهم.

أما تداول البيانات بين أقسام المنظمة مثل قسم الموارد البشرية والمالية وقسم تقنية المعلومات، فلا يشترط أن يُبلّغ أصحاب البيانات بالمشاركات اليومية لبياناتهم لسببين: الأول، أنهم وافقوا على ذلك عند توقيعهم عقود التوظيف بحيث تشمل عقود التوظيف عبارة تنص على مشاركة البيانات الشخصية مع الأطراف ذات الصلة. الثاني، أن هذه الإجراءات تعتبر من الأعمال اليومية المتعارف عليها والمقبولة عرفاً وعقلاً. ويجب التنويه على ماتم ذكره سلفاً في هذه الدراسة، أن من مهام مسؤول حماية البيانات الشخصية أن يساهم في تعزيز الممارسات الإيجابية والصحيحة عند معالجة البيانات الشخصية، لذا فإنه من الضروري عند إرسال ملف يحتوي على بيانات شخصية إلكترونياً بين أقسام المنظمة الواحدة أو خارجها، يجب أن يكون الملف محمي بعبارة سرية يتم إرسالها للمتلقي في وسيلة أخرى. وإن كان ملفاً يدوياً، لابد أن يسلم يداً بيد وأن يتم التحقق من هوية المُستقبِل للملف في كل الأحوال قبل الإرسال.

أما إذا كان الطلب قادماً من جهة أجنبية أو خارج المملكة فلا بد أن يُقيّم من قبل مسؤول حماية البيانات الشخصية وأن يكون من جهة معتمدة وتربطها بالمملكة العربية السعودية علاقات ومصالح سياسية واقتصادية وذات مصداقية عالية. وأن يكون لديها

قانون مُفعّل لحماية البيانات الشخصية. وقد أشارت سياسات حوكمة البيانات الوطنية (2021) إلى إمكانية إرسال البيانات الشخصية إذا لم يكن لدى الجهة الخارجية نظام حماية كافٍ بشرط التقدم بطلب رسمي مكتوب وموافقة أصحاب البيانات الشخصية لأن الهدف ليس عرقلة مصالح الأشخاص، إنما ضبطها والتأكد من سلامتها. ثانياً، لابد أن يبلغ أصحاب البيانات الشخصية ويوافقون على إرسال بياناتهم خارج الحدود. ولا بد أيضاً، وهذا من حققهم، أن يعطوا الفرصة لتحديث بياناتهم قبل الإرسال (سياسات حوكمة البيانات الوطنية،2021). وقد أجاز قانون حماية البيانات الشخصية الأوروبي GDPR في الفقرة 44 إرسال البيانات الشخصية خارج الحدود لكن بشروط وضوابط كتلك التي أشارت إليها السياسات السعودية وشدد القانون على ضرورة الإمتثال وتقديم ما يثبت على القدرة على الحماية عندما تكون هناك حاجة على نقل أو إرسال البيانات الشخصية لبعض مواطني الإتحاد لبلد خارج الإتحاد الأوروبي (EU GDPR, Art. 44). ونظراً لحساسية موضوع نقل البيانات الشخصية لبلد آخر، شدد القانون البريطاني على ضرورة تقديم الضمانات اللآزمة التي تضمن سلامة وصول البيانات الشخصية للأشخاص المعنيين واختيار أنسب الطرق الآمنة لنقل وتلقي البيانات. فالمرسل لابد أن يضمن أمان وسرية نقل المعلومات والمتلقي لا بد أن يؤكد استلامها وكيفية المحافظة عليها (UK GDPR & ICO).

3- البعد الإجرائي

ورد في هذه الدراسة تحت فقرة المبادئ العامة لحماية البيانات الشخصية ضرورة إنشاء سياسة لحماية البيانات الشخصية خاصة لكل منشأة شريطة أن تكون مكتوبة بلغة مفهومة وأن تكون على اتفاق مع السياسة الأم للبلد. ثانياً، أن تقوم المنشأة بتعيين وتوظيف من تراه مناسباً ومؤهلاً لشغل منصب مسؤول حماية البيانات الشخصية ليشرف ويوجه ويصحح الممارسات ويزيد من وعي القوى العاملة بماهية البيانات الشخصية وكيفية التعامل معها ويضمن امتثال الجميع للسياسة المتبعة. وهذا كما ورد آنفاً محل اتفاق بين السياسات الثلاثة (السعودية، البريطانية والأوروبية). وقد فرضت الهيئة السعودية للأمن السيبراني على جميع المنظمات في القطاعين العام والخاص توظيف مختص في الأمن السيراني إلا أن هذا المختص لن يجد الوقت الكافي للنظر في قضايا حماية البيانات الشخصية حيث أنه يرجع في الهرم الإداري الى إدارة تقنية وحماية المعلومات، أما سياسة البيانات الشخصية ترجع الى الإدارة القانونية كونها متطلب قانوني وليس تقني. ومن واقع خبرة في مجال حماية البيانات الشخصية امتدت لخمس سنوات، لا بد أن يكون هناك موظف متفرغ للبيانات الشخصية والقضايا المتعلقة بها ويكون جنباً الى جنب مع مختص الأمن السيراني لتحقيق الهدف الأسمى؛ البيئة الآمنة والمستقبل الآمن. وتعتبر هذه الدراسة هذين الخطوتين – إنشاء السياسة وتعيين موظف مسؤول عن تطبيقها- من أهم وسائل وآليات تطبيق القانون قيد الدراسة وبعدها تأتي الإجراءات التي ستناقش في الفقرات التالية والتي لا يمكن لمسؤول حماية البيانات الشخصية أن يستغني عنها.

3-1 تقييم الآثار المصاحبة لعملية معالجة البيانات الشخصية أو ما يعرف ب: Privacy Impact Assessment (PIA)

من أهم الأدوات المعينة على تحقيق أهداف سياسيات حماية البيانات الشخصية ما يطلق عليه اسم PIA. يجب أن يكون مسؤول حماية البيانات الشخصية موظفاً متفرغاً لها حيث أن العمل يحتاج الى استحداث قاعدة بيانات ومتابعة وتقييم ومراجعة الأسباب الداعية لمعالجة البيانات الشخصية والموازنة بين الإفصاح وعدمه. لم تتكلم السياسة السعودية عن PIA الذي حظي باهتمام بالغ في السياستين الأوروبية والبريطانية. ويعتبر ال PIA من الأدوات التي تساعد على الإمتثال وتُوازن بين الحاجة للبيانات الشخصية من جهه وحمايتها من جهة أخرى وهي عبارة عن إجراء تقييم للتعاملات التي تجري على البيانات الشخصية سواءً يدوياً أو في قواعد البيانات التي تتعامل مع البيانات الشخصية من حفظ، معالجة واسترجاع. والهدف هو اكتشاف المخاطر التي قد تصاحب المعالجة ومن ثم العمل على درئها قبل حدوثها أو التقليل من أثرها السلبي. وتتم عملية التقييم أيضاً عند حاجة المنظمة لتحديث قاعدة البيانات أو توسيع طاقتها الإستيعابية أو عندما يتم استبدالها بنظام جديد (UK ICO & EU GDPR Art.35). في دراسة لآدم ولويديين (2020)، تم بحث دور هذا التقييم PIA بتقييم الآثار والمخاطر التي من الممكن أن تحدث على النساء نتيجة لنظام الرد الآلي الصوتي الذي كان مزودا بصوت نسائي يسهل تمييزه، حيث أن الجدل كان عن إمكانية التعرف على دور ونشاطات النساء في المجتمع من خلال التسجيل الصوتي ومحتواه. والخطر المقدر هو قيام حركة مناهضة، أفراد حزب سياسي، أو تجمع لأشخاص لهم ميول معين ومحاولتهم إلحاق الأذى بالنساء. قيم آدم ولويديين (2020) نظام الرد الصوتي الآلي لكل من Siri, Alexa, and Cortana ومخاطره الإجتماعية مستخدمين PIA. ومن الملاحظات في بحثهما أن أداة التقييم PIA ساعدت كثيرا في التعرف على مكامن الخطر. وأفاد آدم ولويديين (2020) أن التوصيات كانت بأن يعيد جهات التحكم النظر بمنتجاتهم وأن يدرسوا تأثيرها الإجتماعي وأن لا يكون من السهل تمييز جنس الصوت المشغل للرد الآلي.

وقد أسهب مكتب مفوض المعلومات البريطاني، UK ICO، بهذا الصدد لأهميته وتكريسة للممارسات الإيجابية الصحيحة حيث أفاد أن التقييم يجب أن يشتمل على وصف طبيعة معالجة البيانات الشخصية، نطاقها، سياقها، وأسبابها. كما أنه لابد أن لا يُغفل تقييم الحاجة، التناسب، وقياسات الإمتثال. ومن الضروري أيضاً أن تقيس عملية التقييم المخاطر المترتبة على الأشخاص وأن تكون عملية التقييم مشتملة على مقاييس إضافية للتخفيف من آثار المخاطر التي يصعب تجنبها بالكلية. والمخاطر ليست على درجة واحدة من حيث الأثر والضرر الناتج عنها، فمنها ما يكون ضرره بالغ ومنها ما دون ذلك. وهنا يأتي دور مسؤول حماية البيانات الشخصية لقييم عملية معالجة البيانات والمخاطر وإقتراح أنسب الطرق للمحافظة على استمرارية ضمان البيئة الآمنة للبيانات الشخصية (UK ICO).

لا حرج على مسؤول حماية البيانات الشخصية الرجوع الى قائمة الأسئلة التي أدرجها UK ICO لأنها ستوجهه التوجيه الصحيح بشأن مناطق التأثير وكيفية السؤال عنها وتقييمها. وبالمجمل، فإن الأسئلة تدور حول:

1. تحديد الغرض من تقييم PIA

اشرح على نطاق واسع ما يهدف المشروع إلى تحقيقه ونوع المعالجة التي ينطوي عليها. قد تجد أنه من المفيد الرجوع إلى مستندات أخرى داعمة ومفيدة للجواب ، مثل مقترح المشروع. لخص الحاجة إلى تقييم شامل للآثار التي من الممكن أن تصاحب معالجة البيانات.

2. وصف طبيعة الإجراء

وصف طبيعة المعالجة: كيف ستقوم بجمع البيانات واستخدامها وتخزينها وحذفها؟ ما هو مصدر البيانات؟ هل ستشارك البيانات مع أي شخص؟ قد تجد أنه من المفيد الرجوع إلى مخطط تدفق أو طريقة أخرى لوصف تدفقات البيانات. ما هي أنواع المعالجة التي تم تحديدها على أنها تنطوي على مخاطر عالية ومحتملة؟

وصف نطاق المعالجة: ما هي طبيعة البيانات، وهل تشمل بيانات الفئة الخاصة أو الجرائم الجنائية؟ ما مقدار البيانات التي ستجمعها وتستخدمها؟ كم مرة؟ كم من الوقت ستحتفظ به؟ كم عدد الأفراد المتأثرين؟ ما هي المنطقة الجغرافية التي تغطيها؟

وصف سياق المعالجة: ما هي طبيعة علاقتك بالأفراد؟ ما مقدار التحكم الذي سيكون لديهم؟ هل يتوقعون منك استخدام بياناتهم بهذه الطريقة؟ هل تشمل الأطفال أو الفئات الضعيفة الأخرى؟ هل هناك مخاوف سابقة بشأن هذا النوع من المعالجة أو العيوب الأمنية؟ هل هي غريبة وغير اعتيادية بأي شكل من الأشكال؟ ما هو الوضع الحالي للتكنولوجيا في هذا المجال؟ هل هناك أي قضايا حالية تهم الجمهور يجب أن تضعها في الإعتبار؟ هل قمت بالتسجيل في أي مدونة سلوك معتمدة أو نظام إصدار شهادات (حدد إذا حصلت على الموافقة على أي منها)؟

وصف أغراض المعالجة: ما الذي تريد تحقيقه؟ ما هو التأثير المقصود على الأفراد؟ ما هي فوائد المعالجة - بالنسبة لك، وعلى نطاق أوسع

3. الإستشارات

التفكير في كيفية التشاور مع أصحاب المصلحة المعنيين: صف متى وكيف ستسعى للحصول على آراء الأفراد - أو تبرير سبب عدم ملاءمة القيام بذلك. من الذي تحتاج إلى إشراكه داخل مؤسستك؟ هل تحتاج إلى أن تطلب من المساعدة من اي من أصحاب المصلحة؟ هل تخطط للتشاور مع خبراء أمن المعلومات، أو أي خبراء آخرين؟

4. تقييم الضرورة والتناسب

وصف تدابير الامتثال والتناسب، على وجه الخصوص: ما هو الأساس القانوني للمعالجة؟ هل تحقق المعالجة الغرض فعلاً؟ هل هناك طريقة أخرى لتحقيق نفس النتيجة؟ كيف ستمنع تطفل الإدارات الأخرى وتأثيرها السلبي؟ كيف ستضمن جودة البيانات وتقليل البيانات؟ ما هي المعلومات التي ستقدمها للأفراد؟ كيف ستساعدون في دعم حقوقهم؟ ما هي التدابير التي تتخذها لضمان امتثال المساعدين من أصحاب المصلحة؟ كيف يمكنك حماية أي تحويلات دولية؟

5. تحديد وتقييم المخاطر

وصف مصدر المخاطر وطبيعة التأثير المحتمل على الأفراد. تضمين الإمتثال المرتبط بها ومخاطر الشركات حسب الضرورة من حيث احتمال حدوث الضرر، هل هذا الضرر بعيد؟ ممكن أم محتمل؟. شدة الضرر، هل هو ضئيل، يستدعي الإنتباه أو شديد. والمخاطر بالمجمل، هل هي بسيطة، متوسطة أم كبيرة

6. تحديد التدابير اللازمة للحد من المخاطر

حدد التدابير الإضافية التي يمكنك اتخاذها لتقليل المخاطر المحددة على أنها متوسطة أو عالية المخاطر أو القضاء عليها في الخطوة 5

7. تسجيل الخروج وتسجيل النتائج

دمج الإجراءات مرة أخرى في خطة المشروع، مع التاريخ والمسؤولية عن الانتهاء. إذا كان هناك أي مخاطر كبيرة متبقية، فاستشر الجهات التنظيمية أو الجهة المحكمة لسياسة حماية البيانات والمعلومات قبل المضي قدما في تنفيذ المشروع. ويجب على مسؤول حماية البيانات الشخصية تقديم الأرشادات والنصائح الآزمة بشأن الإمتثال وتدابير الخطوة 6 وما إذا كان يمكن المضي قدما في المعالجة (UK ICO).

إن المتأمل لطبيعة هذه الأسئلة سيعلم أن الهدف من طرحها في هذا المجال، هو مواكبة القانون للتقدم العلمي والتقني. ومن واقع خبرة، ليس من المفترض أن يجيب مسؤول حماية البيانات الشخصية على هذه الأسئلة. إنما يكون الإجراء والتصرف السليم لتحقيق الإمتثال بتخاطب الإدارة أو القسم المالك للمشروع مع فريق الحوكمة في المنظمة والذي يعتبر مسؤول حماية البيانات الشخصية جزء منه. لابد أن يشمل الخطاب وصف للمشروع وأهميته ومبررات الحاجة إليه. والهدف من الخطاب هو الحصول على موافقة فريق الحوكمة على المشروع بما انه يتطلب معالجة البيانات الشخصية. بعد أن يدرس مسؤول حماية البيانات الشخصية المشروع الجديد، وعند الشعور بأنه قد يمثل تهديداً، من حيث عدم وضوح آلية معالجة البيانات الشخصية، من يقوم بماذا، ومن يملك ماذا، يطلب فريق الحوكمة من مالك المشروع إكمال النموذج الذي يحتوي على الأسئلة الموضحة في الأعلى. بعد الإجابة عليها من قبل أصحاب المشروع، تعاد مرة أخرى لفريق الحوكمة وبالتحديد، مسؤول حماية البيانات الشخصية ليراجعها ويصدر التوصيات اللازمة والمفترض أنها تصب في مصلحة الإمتثال من غير تحيز للمشروع ولا للجهة المالكة.

2-3 إدارة الحوادث:

إن لم يكن هناك موظف متفرغ أو مسؤول عن حماية البيانات الشخصية لن يكون التعامل مع الحوادث والتسريبات تعاملاً مهنياً يقلل من تأثيرها السلبي ويمنع وقوعها في المستقبل. والهدف من هذه الدراسة كما ذكر سلفاً التعرف على السياسات الدولية ومعرفة ما إذا كانت السياسة المحلية متوافقة والأعراف الدولية. في التعامل مع المخالفات والتجاوزات وعدم التقيد بالأنظمة والقوانين اتفقت السياسات قيد الدراسة على عقوبات مثل الحجز وغرامات مالية رادعة. ففي النظام السعودي لحماية البيانات الشخصية تكلمت المادة الخامسة والثلاثون والسادسة والثلاثون عن عقوبة الإنذار أو الحبس لمدة سنتين والغرامة المالية التي قد تصل الى خمسة ملايين ريال. وألزمت السياسة السعودية لحماية البيانات الشخصية المنظمات بالرد على البلاغات الواردة من أصحاب البيانات الشخصية خلال 72 ساعة (السياسات الأحكام العامة، 4.2.5). والسياستين الأوروبية والبريطانية لم تغفل جانب العقوبات إلا أن لكل سياسة نظام جزائي خاص بها. وربما يتساءل البعض عن أهمية إدارة الحوادث المتعلقة بالبيانات الشخصية، فالإدارة ليست فقط ردود أفعال على المخاطر بعد وقوعها. الإدارة هي وضع خطط متكاملة عن المخاطر واحتمالية حدوثها وكيفية تجنبها، وإن لم يكن تجنبها ممكنا فلا بد من العمل على تقليل أثرها السلبي على الأشخاص وبياناتهم الشخصية. وأيضاً تدوين الدروس المستفادة من الممارسات السابقة لتحسين الممارسات المستقبلية من صميم العمل الإداري. واعتبر دومبرا (2018) في دراسته أن اختراق وتسريب البيانات الشخصية هو في حقيقته اختراق لأنظمة حماية المعلومات بشكل عام ودعى إلى التكامل بين إدارة حماية أمن المعلومات وإدارة حوادث البيانات الشخصية. وأفاد أيضاً، أن هذا التكامل يعزز المستوى الأمني للبيانات (دومبرا، 2018).

وقد ورد تعريف للخروقات في قانون EU GDPR Art.4(12) بأنه خرق للأمن يؤدي إلى تدمير عرضي أو غير قانوني أو فقدان أو تغيير أو الكشف غير المصرح به عن البيانات الشخصية المنقولة أو المخزنة أو المعالجة بطريقة أخرى أو الوصول إليها. وتشمل الخروقات أي فشل أو تعطل لأحد المقاييس الإدارية أو التقنية التي وضعت لتعزيز سبل الحماية. والمزيد من الإيضاح عن ماهية الخروقات والحوادث في مجال البيانات الشخصية في الأمثلة التالية:

1. إرسال بيانات شخصية لأشخاص غير معنيين عن طريق الخطأ. في بعض الأحيان، ونظراً لتشابه الأسماء، تتشابه عناوين البريد الإلكتروني أيضا؛ فيتوهم المرسل أنه يملك بيانات المستلم للبيانات ويقوم بإرسالها دون التحقق بدقة من هوية المرسل إلية، فتكون النتيجة أن البيانات الشخصية أرسلت بالخطأ وعن غير قصد إلى أشخاص غير معنيين
2. الرسائل التي ترسل عبر البريد الإلكتروني لمجموعة من الأشخاص، قد لا يعرف بعضهم الآخر، يتعرف كل منهم على عنوان الآخر بمجرد النظر الى قائمة المرسل لهم إذا لم يكن المُرسل مستخدماً "Bcc".
3. تصفح البيانات الشخصية في أحد أنظمة المنظمة من خلال سوء إدارة التصاريح الازمة. على سبيل المثال، لو أن شخصاً كان يعمل في إدارة الموارد البشرية أو المالية أو أي إدارة أخرى حيث معالجة البيانات الشخصية تتم بشكل يومي، لو أن الشخص انتقل إلى إدارة أخرى لا تعتمد على بيانات شخصية في معاملاتها، يجب أن لا يحتفظ بالتصريح الذي يخولة من تصفح البيانات الشخصية لأنه لم يعد معنياً بذلك.

4. سرقة بعض الأجهزة الإلكترونية
5. حذف وإلغاء البيانات الشخصية الغير مبرر
6. فقد أداة التوثيق والتحقق من الهوية
7. إصابة أيّاً من الأجهزة بعدوى برامج الفدية
8. إتلاف بعض الوثائق أو الأجهزة الإلكترونية المحتوية على بيانات شخصية نتيجة الفيضانات أو الحريق
9. عدم إتباع سياسة الإتلاف الآمن لبعض البيانات التي استوفت الغرض الذي جمعت من أجلة ووجب إتلافها قانونياً (EU GDPR).

1-2-3 المتطلبات القانونية عند الحوادث:

اشتملت توصيات الشيتي (2014) في دراستها على مهام إدرة الحوادث من حيث التفاعل الفوري مع التهديد قبل وبعد وقوعه. كما أن سياسات حوكمة البيانات الوطنية (2021) شددت على عنصر الرد السريع للحوادث والخروقات الأمنية التي تهدد أمن وسلامة البيئة الرقمية. وكان من التعليمات أن التعامل مع الحوادث يبدأ من إبلاغ الجهات التنظيمية فوراً ودون تأخير عند اكتشاف المخالفات بما لا يتجاوز 72 ساعة (السياسات الأحكام العامة، 4.2.5). وهنا يأتي دور مسؤول حماية البيانات الشخصية بتحديث وسائل الإتصال بهذه الجهات التي تتلقي مثل هذه الأنباء ليستفيد من الدعم التي تقدمة الجهات التنظيمية. ويجب على مسؤول حماية البيانات الشخصية أن يسأل نفسه أو تسأل نفسها عن الترتيبات والإجراءات النظامية الإدارية الآزمة التي بذلتها منظمتهم كمحاولة لتفادي هذه الخروقات ويجب أن تكون الإجابات مدعمةُ بالأدلة.

واتفق قانون GDPR مع القانون السعودي على سرعة الإستجابة للحادثة أو الإختراق ونص على عدم تجاوز 72 ساعة من وقت الأختراق. وأوصى GDPR أيضاً، بضرورة إبلاغ أصحاب البيانات المخترقة بما حصل لبياناتهم فوراً ومن دون تأخير ليتسنى لهم أخد الحيطة والحذر واتخاذ الآزم لحماية أنفسهم وأسرهم وممتلكاتهم (GDPR, Recital 86). وإذا كان الإختراق حادثاً في أنظمة الجهات المعالجة أو أحدها، وجب على الجهة المعالجة إبلاغ جهات التحكم فورا.

ومن واقع خبرة في هذا المجال، فإن بعد تلقي خبر الإختراق، يجب على المسؤول عن حماية البيانات الشخصية أن يقوم بعد ذلك بإجراء تقييم لتحديد ما إذا كانت الحادثة تشكل خطراً يستوجب إبلاغ الجهة التنظيمية أو الجهات ذات الصلة أو أصحاب البيانات. للقيام بذلك ، يجب أن يأخذ المسؤول عن حماية البيانات الشخصية في الإعتبار المخاطر المحتملة على الفرد (الأفراد) المعنيين - من حيث شدة التأثير واحتمالية حدوثه. والعوامل التي يجب مراعاتها عند النظر في المخاطر المحتملة: طبيعة وحساسية المعلومات الشخصية المعنية. حجم المعلومات الشخصية المعنية. عدد الضحايا من أصحاب البيانات الشخصية. سهولة تحديد الهوية، أي هل يمكن تحديد أصحاب البيانات الشخصية بواسطة ما تسرب من بيانات؟ أو هل يلزم مطابقتها مع معلومات أخرى؟ مستوى الأمان المطبق على المعلومات الشخصية عند الكشف عنها، على سبيل المثال التشفير أو الاسم المستعار.

يجب على المسؤول عن حماية البيانات الشخصية موازنة الأمور جيداً قبل المضي قدما والتسرع في إبلاغ الجهات المعنية فقد يكون من الممكن إحتواء الأزمة داخلياً وضمان سلامة البيانات الشخصية وأصحابها. على سبيل المثال ، الإفصاح عن طريق الخطأ لأحد الممولين أو المزودين الموثوق بهم من قبل المنظمة أقل خطراً من الكشف إلى مستلم غير معروف أو مستلم بقصد إلحاق الأذى. يجب أيضًا مراعاة ظروف أصحاب البيانات الشخصية. على سبيل المثال، قد يكون مستوى الخطر أكبر إذا كان أصحاب البيانات الشخصية من الأطفال أو البالغين الضعفاء.

وللخطر آثار سلبية عدة يجب على المسؤول عن حماية البيانات الشخصية القدرة على تحديدها وتقديرها. مثلاً: قد يكون الأثر السلبي مادي وقد يكون جسدي أي قد يسبب أضرارا صحية، أو ضرر نفسي من خلال الإضرار بالسمعة. فإذا علم مسؤول البيانات الشخصية ان هذه الأمور ستترتب من علمية الإختراق أو أحدها، وجب علية إتخاذ اللازم في التواصل مع الجهات التنظيمية وأصحاب البيانات الشخصية.

4- النتائج:

اتضح لنا من خلال مقارنة أن هناك اختلاف في المبادئ العامة لحماية البيانات الشخصية في السياسة السعودية عن نظيراتها البريطانية والأوروبية. وهذا الإختلاف ناشئ عن عدم تضمن السياسة السعودية مبدأ الخصوصية من مراحل التصميم Privacy in Design and Default. كما أن المقارنة بينت لنا أن السياسة السعودية لم تتكلم عن أداة مهمة في تقييم الأثر المترتب على الخصوصية جراء المعالجة اليومية للبيانات الشخصية وهذه الأداة تعرف ب Privacy Impact Assessment. تمكن هذه الأداة المسؤولين عن حماية

البيانات الشخصية من اكتشاف المخاطر التي قد تصاحب عملية معالجة البيانات الشخصية باكراً ومن ثم رسم الخطط المخاطر بما يخدم المصالح العامة للمنظمات.

ومما لوحظ أثناء دراسة السياسات الثلاثة الإجماع على أن تكون لكل منظمة سياسة خاصة بها تنظم معالجة البيانات الشخصية وأن يكون هناك مسؤول مكلف بشكل كامل عن إدارة البيانات الشخصية وضمان الإمتثال للسياسات المقرة. إلا أن هذه المرحله لاتزال في بواكيرها في المملكة العربية السعودية نظراً لحداثة كل من سياسة حماية البيانات الشخصية والأمن السيبراني.

ومن واقع خبرة في مجال حماية البيانات الشخصية في إحدى الشركات البريطانية، أستطيع القول بأن حماية البيانات الشخصية متطلب قانوني بينما الأمن السيبراني متطلب تقني وفني ويرجع بطبيعة الحال الى تقنية وأمن المعلومات وفي بعض المنظمات وبسبب حساسيته يرجع الى الإدارة العليا. على سبيل المثال، قبل عشر سنوات كانت حماية البيانات الشخصية في الشركة البريطانية التي أعمل بها جزءً من سياسة الحماية Security policy. ومنذ 2014 تقريباً أصبحت سياسة حماية البيانات سياسة مستقلة قائمة بحد ذاتها.

5- الخاتمة:

أجابت هذه الورقه على التساؤلات البحثية المتعلقة بنظام أو سياسة حماية البيانات الشخصية وعرفت القارئ الكريم بماهية البيانات الشخصية، جهات التحكم، الجهات المعالجة والمعالجة العادلة للبيانات الشخصية. كما ذكرت هذه الورقة فوائد نظام حماية البيانات الشخصية على الفرد والمجتمع في الداخل السعودي وفي الخارج. وبعد المقارنة بين السياسات، سلطت هذه الورقة الضوء على أوجه التشابه والإختلاف. ومما توصلت إلية هذه الدراسة عند الحديث عن البعد القانوني إجماع السياسات قيد الدراسة على ضرورة توافر سياسة حماية بيانات شخصية لكل منظمة وأن يكون شخص مسؤول عن إدارتها. كان هناك إجماع على أن لأصحاب البيانات الشخصية حقوق يجب على المنظمات احترامها. وإجماع على المعالجة العادلة للبيانات الشخصية بما في ذلك مشاركة البيانات مع الغير.

في البعد القانوني من هذه الورقة ونظراً لحداثة السياسة السعودية، لم تغطي السياسة السعودية جانب Privacy in Design and Default الذي يهتم بإدراج الخصوصية منذ مراحل التصميم الأولى لقواعد البيانات التي تعالج البيانات الشخصية. وفي البعد الإجرائي، لم تذكر السياسة السعودية أداة مهمة من أدوات تقييم الآثار المترتبة علة الخصوصية نتيجة لمعالجة البيانات الشخصية بشكل يومي. وهذه الأداة مشدد عليها في القانونين البريطاني والأوروبي وهي Privacy Impact Assessment. وفي البعد الإجرائي أيضاً، ثمة إجماع على آلية التعامل مع الحوادث وخرق الأنظمة المتعلقة بسياسة حماية البيانات الشخصية

هذه الدراسة توصي المشرع في المملكة العربية السعودية بالتركيز على حماية البيانات الشخصية بشكل أكبر وجعله مستقلاً وإرسال رسائل لجميع المنظمات في القطاعين العام والخاص قوية بالإسراع في إنشاء السياسات المتعلقة وتقديم ضمانات للإمتثال منها على سبيل المثال تعيين مسوول يراقب ويوجه جميع العاملين عل كيفية التعامل مع البيانات الشخصية لأن هذا يصب أيضا في خانة الأمن السيبراني ولا يتعارض معه على الإطلاق حتى إن اختلفت المرجعيات.

من الدراسات المستقبيلة، دراسة إحصائية توضح أعداد المنظمات الحكومية الممتثلة لقانون حماية البيانات الشخصية من خلال إنشاء سياسة خاصة وتوظيف مسؤول عنها وبحث أسباب عدم امتثال المنظمات الأخرى وتقديم الحلول لفرض واقع أفضل وأكثر أماناً.

المراجع العربية:

- أحمد، ه. (2017). قانون حماية البيانات الشخصية فى مواقع التواصل الاجتماعى لمؤسسات المكتبات والمعلومات: دراسة تحليل مضمون .المؤتمر الثامن والعشرون: شبكات التواصل الاجتماعي وتأثيراتها في مؤسسات المعلومات في الوطن العربي، القاهرة: الاتحاد العربى للمكتبات والمعلومات (اعلم)، 1 - 25. مسترجع منhttp://search.mandumah.com/Record/853921
- الشيتي، إ.م. (2014). تقييم سياسات أمن وخصوصية المعلومات في المؤسسات التعليمية في المملكة العربية السعودية .مجلة الجمعية المصرية لنظم المعلومات وتكنولوجيا الحاسبات14 ,(الرابع عشر)، 11-24 doi: 10.21608/jstc.2014.119253
- حوكمة سياسات البيانات الحكومية الإصدار الثاني تاريخ 2021/05/26. مكتب إدارة البيانات الوطنية. مسترجع من sdaia.gov.sa بتاريخ 2023/05/18
- ضوابط ومواصفات إدارة البيانات الوطنية وحوكمتها وحماية البيانات الشخصية (يناير، 2021). مسترجع (2023) من مكتب إدارة البيانات الوطنية: Policies001.pdf (sdaia.gov.sa)

- علي، م.ع. (2021). النظام القانوني لحماية البيانات الشخصية المعالجة إلكترونيا: دراسة تحليلية مقارنة في ضوء اللائحة الأوربية وبعض التشريعات ذات العلاقة .مجلة العلوم القانونية، مج7، ع14 ، 73 .118 - مسترجع من http://search.mandumah.com/Record/1197076
- غالب، ع.و. (2019). قانون حماية البيانات الشخصية .مجلة الإقتصاد الإسلامي العالمية، ع87 ، 50-54 مسترجع من http://search.mandumah.com/Record/1064265
- نظام حماية البيانات الشخصية رقم (م/148) بتاريخ 1444/9/5. مسترجع (2023) من الهيئة السعودية للبيانات والذكاء الإصطناعي: الأنظمة واللوائح(sdaia.gov.sa)

المراجع الأجنبية:

- Cooper, D., & Lensdorf, L. (2022). EDPB Draft Guidelines 01/2022 on Data Subject Rights–Right of Access: The draft guidelines of the European Data Protection Board on the data subject's access rights in the light of the consultation phase. *Computer Law Review International*, *23*(3), 65-70.
- Dombora, S. (2018). Integrated incident management model for data privacy and information security. In *BOOK OF PROCEEDINGS* (p. 319).
- Hofman, D., Duranti, L., & How, E. (2017). Trust in the balance: Data protection laws as tools for privacy and security in the cloud. *Algorithms*, *10*(2), 47.
- EU GDPRretreived from GDPR: https://gdpr.eu/taq/gdpr on 31/07/2023 G20 retreived from https://www.g20.org/en/ .on 01/08/2023
- Zhang, J., Hassandoust, F., & Williams, J. E. (2020). Online customer trust in the context of the general data protection regulation (GDPR). *Pacific Asia Journal of the Association for Information Systems*, *12*(1), 4.
- Taylor, L., Floridi, L., & Van der Sloot, B. (Eds.). (2016). *Group privacy: New challenges of data technologies* (Vol. 126). Springer.
- Floridi, L. (2013). *The ethics of information*. Oxford University Press, USA.
- Saggi, M. K., & Jain, S. (2018). A survey towards an integration of big data analytics to big insights for value-creation. *Information Processing & Management*, *54*(5), 758-790.
- Loideain, N. N., & Adams, R. (2020). From Alexa to Siri and the GDPR: the gendering of virtual personal assistants and the role of data protection impact assessments. *Computer Law & Security Review*, *36*, 105366.
- Najim Al-Shammari .(2019) .E-Commerce in Saudi Arabia: Characteristics of Trustworthy Usable E-commerce Wbsites . *Internation Journal of Information Science, 6-15.*
- Personal Data Protection retreived from Information Comissioner's Office: https://ico.org.uk on 01/08/2023
- Saudi Vission 2030 retreived from Homepage: The Progress & Achievements of Saudi Arabia - Vision 2030 on 01/08/2023
- Schwartz, P. M. (2021). The Data Privacy Law of Brexit: Theories of Preference Change. *Theoretical Inquiries in Law*, *22*(2), 111-152.