

حماية خصوصية بيانات المستفيدين في المكتبات الأكاديمية العربية والعالمية : القوانين والسياسات
مستلة من رسالة دكتوراه بعنوان : حماية خصوصية بيانات المستفيدين في المكتبات الأكاديمية بمصر
: دراسة ميدانية

مراجعة وإشراف
أ.د. سلوى السعيد
أستاذ المكتبات والمعلومات
بكلية الآداب جامعة القاهرة
salwaa@squ.edu.om

إعداد
ندا لبيب مصطفى
المكتبة المركزية بجامعة مصر للعلوم
والتكنولوجيا
nada.labib@must.edu.eg

المخلص

تناولت الدراسة قوانين وتشريعات خصوصية البيانات الشخصية عربيًا وعالميًا مستخدمة المنهج المسحي وتأثيرها في سياسات الخصوصية المُتبعة في المكتبات الأكاديمية عربيًا وعالميًا، مع التركيز على قانون حماية البيانات الشخصية المصري رقم ١٥١ لعام ٢٠٢٠ وتبيان مدى الاتفاق والاختلاف بينه وبين اللائحة العامة لحماية البيانات الشخصية GDPR لعام ٢٠١٦ والصادرة عن الاتحاد الأوروبي؛ من حيث الإطار المفاهيمي لقانون حماية البيانات الشخصية، وحقوق الشخص المعني بالبيانات وشروط المعالجة، وأخيرًا وسائل إنفاذ قانون حماية البيانات الشخصية، ودراسة لسياسات الخصوصية بالمكتبات الأكاديمية للجامعات عربيًا وعالميًا.

وُسمت الدراسة **طبقًا للدول** إلى قوانين حماية خصوصية البيانات عربيًا وتشمل: جمهورية مصر العربية، والمملكة الأردنية الهاشمية، والإمارات العربية المتحدة، والمملكة العربية السعودية، وتونس، والمملكة المغربية، وقطر؛ وعالميًا وتشمل: الولايات المتحدة الأمريكية ودول الاتحاد الأوروبي والمملكة المتحدة على الرغم من خروجها من الاتحاد الأوروبي في الأول من فبراير ٢٠٢٠.

وطبقًا لسياسات الخصوصية بالمكتبات قسمت الدراسة السياسات إلى سياسات الخصوصية عربيًا وتشمل: المملكة العربية السعودية .. سياسات الخصوصية بمكتبات جامعة الجوف، ومكتبة جامعة الملك فيصل، وسلطنة عمان .. سياسات خصوصية جامعة الملك قابوس، وقطر .. سياسات خصوصية مكتبة قطر الرقمية، ولبنان .. سياسات خصوصية مكتبات الجامعة الأمريكية في بيروت، وفلسطين .. سياسات خصوصية مكتبة جامعة القدس المفتوحة، وسياسات الخصوصية عالميًا وتشمل: الولايات المتحدة الأمريكية .. سياسات خصوصية مكتبات جامعة بيتسبرج، ومكتبة جامعة هارفارد، ومكتبة جامعة بيركلي بكاليفورنيا، وكندا .. سياسات خصوصية مكتبة جامعة ماكجيل، وأستراليا .. سياسات مكتبة جامعة نيو ساوث ويلز سيدني.

رَتبت الدراسة الدول تحت كل قطاع – عربيًا وعالميًا - زمنيًا من الأقدم إلى الأحدث من حيث سن القوانين والعمل بها. لتعرض الدراسة بعد ذلك الفروقات ما بين قانون حماية البيانات الشخصية المصري رقم ١٥١ لعام ٢٠٢٠ واللائحة العامة لحماية البيانات الشخصية **General Data Protection Regulation** والصادرة عن الاتحاد الأوروبي؛ لرصد أوجه التشابه والاختلاف في بعض الجوانب مثل: الإطار المفاهيمي لقانون حماية البيانات الشخصية، وحقوق الشخص المعني بالبيانات وشروط المعالجة، والتزامات أطراف معالجة وحماية البيانات، ووسائل إنفاذ قانون حماية البيانات الشخصية، لتنتهي بعرض نماذج لبعض سياسات حماية الخصوصية المعمول بها في المكتبات الأكاديمية بالجامعات عربيًا وعالميًا.

الكلمات المفتاحية: سياسات الخصوصية في المكتبات الأكاديمية، قوانين حماية خصوصية البيانات، تشريعات حماية خصوصية البيانات، أمن البيانات، الكود الأخلاقي للمكتبات.

١/ التمهيدي:

إن حرية تداول المعلومات وحرية التعبير واللذين تنص عليهما المادة ١٩ من الإعلان العالمي لحقوق الإنسان، ميدان أساسيان في مهنة المكتبات والمعلومات، وتعد الخصوصية جزء لا يتجزأ من هذه الحقوق والخصوصية في المكتبات ومراكز المعلومات ضرورية عند التعامل معهما، بحيث تتيح لمستخدمي المكتبة استخدام المعلومات والأفكار والوصول إليها والإطلاع عليها دون خوف من الإحراج أو الحكم أو العقوبة أو انتهاك الخصوصية. حيث يمكن لانتهاك الخصوصية أن يؤثر تأثيرًا سلبيًا على رغبة مستخدمي المكتبة في زيارة المكتبات ومراكز المعلومات، مما يؤثر بشكل كبير على حرية الوصول إلى الأفكار والتعامل مع المكتبة بشكل خاص خوفًا من الانتهاك، حيث يتطلب التعامل مع المكتبات توافر حرية استخدام المكتبة بناءً على عنصرين وهما: الاختيار من مجموعة متنوعة من المواد، والتأكد من عدم مراقبة خيارات الشخص، وفي سياق ذلك يقع على عاتق المكتبات وأمناء المكتبات والعاملين في المكتبات التزام أخلاقي، مُعبر عنه بوضوح في قواعد أخلاقيات جمعية المكتبات الأمريكية ALA وذلك للحفاظ على حق المستخدمين في الخصوصية ومنع أي استخدام أو كشف غير مصرح به لمعلومات التعريف الشخصية للمستخدمين أو البيانات المرتبطة باستخدامهم لموارد المكتبة، ويشمل ذلك اعتماد سياسات وممارسات تُعامل بيانات المستفيد على أنها سرية. (ALA Statements and Policies,2017)

وعليه تناولت الدراسة مستخدمة المنهج المسحي قوانين حماية البيانات الشخصية عربيًا وعالميًا وتأثيرها في سياسات الخصوصية المُتبعة في المكتبات الأكاديمية عربيًا وعالميًا، مع التركيز على قانون حماية البيانات الشخصية المصري رقم ١٥١ لعام ٢٠٢٠ وتبيان مدى الاتفاق والاختلاف بينه وبين اللائحة العامة لحماية البيانات الشخصية GDPR لعام ٢٠١٦ والصادرة عن الاتحاد الأوروبي؛ من حيث الإطار المفاهيمي لقانون حماية البيانات الشخصية، وحقوق الشخص المعني بالبيانات وشروط المعالجة، وأخيرًا وسائل إنفاذ قانون حماية البيانات الشخصية، ودراسة لسياسات الخصوصية بالمكتبات الأكاديمية للجامعات عربيًا وعالميًا.

حدود الدراسة:

فُسمت الدراسة **طبقًا للدول** إلى قوانين حماية خصوصية البيانات عربيًا وتشمل: جمهورية مصر العربية، والمملكة الأردنية الهاشمية، والإمارات العربية المتحدة، والمملكة العربية السعودية، وتونس، والمملكة المغربية، وقطر؛ وعالميًا وتشمل: الولايات المتحدة الأمريكية ودول الاتحاد الأوروبي والمملكة المتحدة على الرغم من خروجها من الاتحاد الأوروبي في الأول من فبراير ٢٠٢٠، أو ما يعرف باسم البريكست^١ Brexit (خميس؛ الطيار، ٢٠٢١).

وطبقًا لسياسات الخصوصية بالمكتبات قسمت الدراسة السياسات إلى سياسات الخصوصية عربيًا وتشمل: المملكة العربية السعودية .. سياسات الخصوصية بمكتبات جامعة الجوف، ومكتبة جامعة الملك فيصل، وسلطنة عمان .. سياسات خصوصية جامعة الملك قابوس، وقطر .. سياسات خصوصية مكتبة قطر الرقمية، ولبنان .. سياسات خصوصية مكتبات الجامعة الأمريكية في بيروت، وفلسطين .. سياسات خصوصية مكتبة جامعة القدس المفتوحة، وسياسات الخصوصية عالميًا وتشمل: الولايات المتحدة الأمريكية .. سياسات خصوصية مكتبات جامعة بيتسبرج، ومكتبة جامعة هارفارد، ومكتبة جامعة بيركلي بكاليفورنيا، وكندا .. سياسات خصوصية مكتبة جامعة ماكجيل، وأستراليا .. سياسات مكتبة جامعة نيو ساوث ويلز سيدني.

رَتَبَت الدراسة الدول تحت كل قطاع – عربيًا وعالميًا - زمنياً من الأقدم إلى الأحدث من حيث سن القوانين والعمل بها. لتعرض الدراسة بعد ذلك الفروقات ما بين قانون حماية البيانات الشخصية المصري رقم ١٥١ لعام ٢٠٢٠ واللائحة العامة لحماية البيانات الشخصية **General Data Protection Regulation** والصادرة عن الاتحاد الأوروبي؛ لرصد أوجه التشابه والاختلاف في بعض الجوانب مثل: الإطار المفاهيمي لقانون حماية البيانات الشخصية، وحقوق الشخص المعني بالبيانات وشروط المعالجة، والتزامات أطراف معالجة وحماية البيانات، ووسائل إنفاذ قانون حماية البيانات الشخصية، لتنتهي بعرض نماذج لبعض سياسات حماية الخصوصية المعمول بها في المكتبات الأكاديمية بالجامعات عربيًا وعالميًا.

أهمية الدراسة:

تتلخص أهمية الدراسة في رصد قوانين وتشريعات خصوصية البيانات الشخصية ومدى تأثيرها على سياسات الخصوصية في المكتبات عربيًا وعالميًا.

الاستشهادات المرجعية:

اتبعت الدراسة أسلوب صياغة الاستشهادات المرجعية التابع لجمعية علم النفس الأمريكية APA .STYLE

١/١ قوانين حماية خصوصية البيانات عربيًا:

• تونس (قانون رقم ٦٣ لسنة ٢٠٠٤ والمتعلق بحماية المُعطيات الشخصية) :

تُعتبر وزارة العدل هي الجهة المسؤولة عن إصدار القانون، حيث يأتي القانون في سبعة أبواب مقسمة إلى ١٠٥ فصلاً (مادة)، حيث يبدأ الباب الأول بأحكام عامة توضح في البداية "أن لكل شخص الحق في حماية المعطيات (البيانات) الشخصية المتعلقة بحياته الخاصة باعتبارها من الحقوق الأساسية المضمونة بالدستور" ليتدرج بعد ذلك في توضيح لأنواع المعالجة التي تتم على البيانات، ثم يعرض للمفاهيم والمصطلحات الخاصة بالقانون مثل: معالجة المعطيات الشخصية، المعني بالأمر، المناول، الإحالة، الربط البيني. ويشرح الباب الثاني شروط المعالجة والإجراءات الأولية للحصول على البيانات مثل الحصول على تصريح مسبق يودع بمقر الهيئة الوطنية لحماية المعطيات الشخصية، ثم يناقش القانون المسؤول عن معالجة المعطيات الشخصية وواجباته ومن ضمن شروط المعالجة الواردة في نص القانون أنه " لا يجوز ربط إساءة خدمة أو منفعة لفائدة شخص بشرط موافقته على معالجة معطياته الشخصية، أو استغلالها في غير الأغراض التي جمعت من أجلها" وهو ما يتفق مع أهمية الحفاظ على خصوصية الأشخاص وعدم إساءة استخدام بياناتهم الشخصية في غير الأغراض التي جُمعت لأجلها أو مساومتهم على بياناتهم.

اشتراط القانون أيضًا أن يكون القائم على معالجة البيانات الشخصية تونسي الجنسية ومقيم داخل حدود الدولة التونسية، ولا يمكن إعادة استخدام البيانات الشخصية للأفراد إلا في حالتين وضحه المشرع: الحالة الأولى إذا كانت تلك البيانات صالحة لأن تستخدم في أغراض تاريخية أو علمية، والثانية أن القائم على المعالجة تغير وتقرر إحالة البيانات إلى شخص آخر ليتابع عملية المعالجة؛ وفي هذه الحالة لا يتم ذلك إلا بعد الحصول على موافقة كتابية من المعني بالأمر بنفسه أو أحد ورثته في حالة وفاته. وفيما يخص حق النفاذ أو الوصول وضح القانون بأنه لا يمكن التنازل مسبقًا عن حق النفاذ أو الوصول، وفيما يخص العقوبات أوضح القانون أن العقوبة تتراوح ما بين سنتين إلى خمس سنوات وغرامة من خمسة آلاف إلى خمسين ألف دينار.

← تونس. وزارة العدل. الهيئة العامة لحماية المعطيات الشخصية. قانون رقم ٦٣ لسنة ٢٠٠٤ والمتعلق بحماية المعطيات الشخصية: <https://bit.ly/3Ofcvo2>.

• المملكة المغربية (قانون رقم ٠٩,٠٨ لسنة ٢٠٠٩ والمتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي):

مديرية التشريع بوزارة العدل هي الجهة المسؤولة عن إصدار القانون، ويتكون القانون من ثمانية أبواب وعدد ٦٧ مادة تبدأ بالمفاهيم والتعريفات الواردة في بداية نص القانون؛ إلا أنه وضح نوع المعالجة الخاضعة لتطبيق القانون؛ وهي المعالجة الآلية سواء كانت كلية أو جزئية؛ كذلك المعالجة غير الآلية ويقصد بها التقليدية، أيضاً اتفق القانون المغربي مع التونسي في ضرورة أن يكون القائم على المعالجة مغربي الجنسية وأن تتم المعالجة على الأراضي المغربية، وحدد المشرع أن تعالج البيانات بطريقة نزيهة ومشروعة، وأن تكون ملائمة ومناسبة وغير مفرطة، وتحتوي على بيانات صحيحة غير مُضللة، محفوظة وفق شكل يمكن من التعرف على الأشخاص المعنيين طوال مدة لا تتجاوز المدة الضرورية لإنجاز الغايات التي تم جمعها ومعالجتها لاحقاً من أجلها؛ كذلك لا يمكن القيام بعمليات المعالجة على البيانات بدون موافقة كتابية من الشخص المعني توضح رضاه عن عملية المعالجة بالكامل، وهناك حق آخر مكفول للشخص المعني بالبيانات وهو الحق في الولوج حيث حدد المشرع بأنه يحق للشخص المعني - بعد الإلقاء بما يثبت هويته - أن يحصل من المسؤول عن المعالجة بمعلومات عن البيانات التي يتم معالجتها وحالتها ووضح ماهية البيانات بالضبط الخاضعة للمعالجة، ومنه انتقل القانون للحق في التصحيح؛ وهو حق الشخص المعني بأن يقدم طلب لتصحيح بيانات معينة أو تعديلها أو حذفها من خلال طلب يقدم من الشخص ذاته، كذلك للشخص المعني سلطة التحكم في إتلاف أو تغيير البيانات أو مراقبة انتقالها عبر الخادمت Servers داخل حدود الوطن؛ كما أشار التشريع المغربي لحماية البيانات على أنه في حالة النقل البيئي للبيانات بين الدول؛ أن تكون الدولة المنقول لها البيانات تضمن مستوى حماية كاف للحياة الشخصية وللحريات والحقوق للأشخاص إزاء المعالجة التي تخضع لها هذه البيانات أو قد تخضع لها. وتتراوح العقوبات ما بين سحب ترخيص الحصول على البيانات الشخصية؛ لتصل إلى الغرامة ما بين ١٠٠٠٠ آلاف درهم إلى ٢٠٠٠٠٠ درهم.

← المملكة المغربية. وزارة العدل. مديرية التشريع. قانون رقم ٠٩,٠٨ لسنة ٢٠٠٩ والمتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي. <https://bit.ly/3QlgK3d>

• المملكة الأردنية الهاشمية (مشروع قانون حماية البيانات الشخصية لسنة ٢٠١٤):

يصدر عن وزارة الاتصالات الأردنية ويُعرف باسم قانون حماية البيانات الشخصية؛ قسم إلى أربعة أقسام يشتمل القسم الأول على المفاهيم واكتفى القانون بتعريف مصطلحين وهما: "البيانات الشخصية" حيث عرفها بأنها "أي معلومات خاصة بشخص طبيعي قابل للتعرف عليه"، ومصطلح "البيانات الحساسة" وهي البيانات المتعلقة بالعرق والديانة والمعتقدات والسجل الإجرامي؛ وتختلف خطورتها وأهميتها عن البيانات الأساسية مثل الاسم، تاريخ الميلاد والعنوان، إذ تتطلب بعض البيانات حماية أكبر من غيرها، والقسم الثاني وتشمل حقوق صاحب البيانات؛ وتختص بالموافقات على العمليات التي تتم على البيانات، وشروط الموافقة، وحق صاحب البيانات بالاطلاع على بياناته، وتعديلها وحذفها، والقسم الثالث وهو التزامات الجهة التي تتعامل مع البيانات، في حالة مشاركة البيانات بين الجهات المختلفة، ومشاركة البيانات عبر الحدود، والحد من مدة احتجاز البيانات، ثم يأتي القسم الرابع والأخير والذي يختص بوسائل تنفيذ القانون من حيث تشكيل ما يعرف باسم مجلس للخصوصية لمراقبة العمليات التي تتم على البيانات، والفصل في النزاعات حول عمليات البيانات، ويحتوي أيضاً القسم الأخير على الاحتياطات الأمنية، وآلية الخطر في حالة التعرض لانتهاكات وخروقات. (حموري؛ المصري، ٢٠١٤)

والذي أدى إلى صدور قانون حماية البيانات الشخصية لسنة ٢٠٢٠ بعد ست سنوات من عرض مشروع القانون.

← المملكة الأردنية الهاشمية. ديوان التشريع والرأي. قانون حماية البيانات الشخصية لسنة ٢٠٢٠. <https://bit.ly/3Hx8oBu>

• الإمارات العربية المتحدة :

مبادرة بيانات دبي ٢٠١٥ :

تم إطلاق مبادرة بيانات دبي في سنة ٢٠١٥ في إطار سياسة حكومة دبي الرامية إلى تطوير ثقافة تبادل البيانات واتخاذ القرارات المستندة إلى الأدلة بين الجهات المختصة الحكومية والخاصة.

ووضعت المبادرة ١١ هدفا استراتيجياً لتبادل البيانات والابتكار، وفق ثلاثة مبادئ رئيسية تتعلق باستخدام وإعادة استخدام البيانات، وحماية خصوصية المعلومات السرية، وحماية الملكية الفكرية. وتتمثل هذه الأهداف الاستراتيجية فيما يلي:

١. تمكين الإمارة من تحقيق رؤيتها في جعل دبي أسعد مدينة.
٢. إدارة بيانات دبي وفق منهجية واضحة ومحددة، تتفق مع أفضل الممارسات العالمية.
٣. تحقيق التناغم والتكامل بين الخدمات التي تقدمها الجهات الحكومية الاتحادية والجهات الحكومية المحلية.
٤. الاستفادة المثلى من البيانات المتوفرة لدى مزودي البيانات.
٥. تعزيز الشفافية وإرساء قواعد الحوكمة بشأن نشر وتبادل البيانات.
٦. زيادة كفاءة الخدمات التي تقدمها الجهات الحكومية الاتحادية والجهات الحكومية المحلية، من حيث مستوى الجودة، وسرعة الإنجاز، وتبسيط الإجراءات وتخفيض كلف التشغيل.
٧. زيادة القدرة التنافسية لمزودي البيانات، ورفع مؤشر تنافسية دولة الإمارات العربية المتحدة على المستوى الدولي.
٨. دعم عملية اتخاذ القرار لدى الجهات الحكومية الاتحادية والجهات الحكومية المحلية، وتمكينها من إعداد سياساتها وتنفيذ خططها ومبادراتها الاستراتيجية بكفاءة وفعالية.
٩. ترسيخ ثقافة الإبداع، والإسهام في دعم المبادرات الابتكارية التي من شأنها تأمين رفاهية العيش للمقيمين والزوار.
١٠. تحقيق التوازن بين عملية نشر وتبادل المعلومات، والحفاظ على سربيتها وخصوصيتها.
١١. توفير البيانات اللازمة للجهات غير الحكومية بهدف دعم الخطط التنموية والاقتصادية في الإمارة.

وترتكز الاستراتيجية على ١٣ مبدأ موزعة على ثلاثة محاور وهي:

١. نشر ومشاركة البيانات.
٢. استخدام البيانات وإعادة استخدامها.
٣. الخصوصية، والموثوقية، والملكية الفكرية

← الإمارات العربية المتحدة. حكومة دبي. قانون بيانات دبي. مبادرة بيانات دبي. <https://www.digitaldubai.ae/ar/data>

القانون الاتحادي رقم ١٢ لسنة ٢٠١٦ لحماية البيانات والخصوصية:

تُطبق دولة الإمارات القانون الاتحادي رقم (١٢) لسنة ٢٠١٦ وتُعتبر وزارة العدل هي الجهة المسؤولة عن إصداره، حيث قامت بتعديل المرسوم بقانون اتحادي رقم (٥) لسنة ٢٠١٢ في شأن مكافحة جرائم تقنية المعلومات، وغيره من القوانين المتعلقة بحماية الخصوصية، ومنع انتهاك البيانات الشخصية؛ حيث تحظر المادة ٢١ من القانون استخدام شبكة معلوماتية، أو نظام معلومات إلكتروني، أو إحدى وسائل تقنية المعلومات، في الاعتداء على خصوصية شخص في غير الأحوال المصرح بها قانوناً بإحدى الطرق التالية: استراق السمع، أو اعتراض، أو تسجيل أو نقل أو بث أو إفشاء محادثات أو اتصالات أو مواد صوتية أو مرئية، أو التقاط صور الغير أو إعداد صور إلكترونية أو نقلها أو كشفها أو نسخها أو الاحتفاظ بها، أو نشر أخبار أو صور إلكترونية أو صور فوتوغرافية أو مشاهد أو تعليقات أو بيانات أو معلومات ولو كانت صحيحة وحقيقية.

كما تحظر المادة ٢٢ من القانون كل من استخدم بدون تصريح، أي شبكة معلوماتية، أو موقعاً إلكترونيًا، أو وسيلة تقنية معلومات لكشف معلومات سرية حصل عليها بمناسبة عمله أو بسببه.

كما وتلتزم المؤسسات والشركات في دولة الإمارات العربية المتحدة التي تستخدم البيانات الشخصية لمواطني الاتحاد الأوروبي باللائحة العامة لحماية البيانات (GDPR)، والذي تم تطبيقها بالفعل اعتباراً من ٢٥ مايو ٢٠١٨.

وهو ما فعلته المملكة المتحدة على الرغم من انفصالها عن الاتحاد الأوروبي إلا أنها التزمت باللائحة العامة لحماية البيانات والخاصة بدول الاتحاد الأوروبي، وذلك لارتباطها بالعديد من الاتفاقيات والعقود التجارية المُلزِمة خضوعها لسياسات لائحة الاتحاد الأوروبي.

← الإمارات العربية المتحدة. وزارة العدل. القانون الاتحادي رقم ١٢ لسنة ٢٠١٦ لحماية البيانات والخصوصية. <https://bit.ly/3ER9Opi>

• قطر (قانون رقم ١٣ لسنة ٢٠١٦ بشأن حماية خصوصية البيانات الشخصية):

يأتي القانون القطري بشأن حماية خصوصية البيانات الشخصية لعام ٢٠١٦ والصادر عن وزارة المواصلات والاتصالات في ثمانية فصول؛ كما في القوانين السابقة يبدأ الفصل الأول بالمصطلحات والمفاهيم العامة التي لم تختلف عن سابقتها إلا ورود فقرة في الفصل الأول توضح حدود سريان أحكام القانون ورد فيها: "تسري أحكام هذا القانون على البيانات الشخصية عندما تتم معالجتها على نحو إلكتروني، أو يتم الحصول عليها أو جمعها أو استخراجها على أي نحو آخر تمهيداً لمعالجتها إلكترونياً، أو تتم معالجتها عن طريق الجمع بين المعالجة الإلكترونية والمعالجة التقليدية"، جاءت المادة الخامسة في الفصل الثاني لتوضح حقوق الفرد في:

- ١- سحب موافقته السابقة على معالجة بياناته الشخصية.
- ٢- الاعتراض على معالجة بياناته الشخصية إذا كانت غير ضرورية لتحقيق الأغراض التي جمعت من أجلها، أو كانت زائدة على متطلباتها، أو تمييزية أو مجحفة أو مخالفة للقانون.
- ٣- طلب حذف بياناته الشخصية أو محوها في الحالات المشار إليها في البندين السابقين، أو عند انتهاء الغرض الذي تمت من أجله معالجة تلك البيانات، أو إذا لم يكن هناك مبرر للاحتفاظ بها لدى المراقب.
- ٤- طلب تصحيح بياناته الشخصية، مرفقاً به ما يثبت صحة طلبه؛ كإثبات للشخصية؛ أو أوراق تثبت تغيير البيانات.

ويأتي الفصل السادس من القانون بعنوان "الاتصالات الإلكترونية بغرض التسويق المباشر" ليوضح حظر إجراء أي اتصال إلكتروني بغرض التسويق المباشر إلى الفرد، إلا بعد الحصول على موافقته المسبقة؛ وهو ما يجب تطبيقه عند تفعيل سياسات الخصوصية في المكتبات، حيث يجب على القائمين على تقديم خدمات المكتبة الفصل ما بين البيانات التي تُسجل للحصول على خدمات المكتبة كخدمة الإعارة أو الخدمة المرجعية، وما بين موافقة الفرد بصورة واضحة ومباشرة على استقبال رسائل البريد الإلكتروني أو الاتصالات الهاتفية من أجل التسويق لهذه الخدمات عن طريق استخدام بياناته المُسجلة لغير هذا الغرض.

ويوضح الفصل السابع من القانون العقوبات والتي تراوحت بين غرامة مليون ريال إلى خمسة ملايين لكل من خالف أحكام المواد الموضحة بالقانون، ويأتي الفصل الثامن والأخير بمجموعة من الأحكام الختامية والتي تضطلع بتقديم الشكاوى، وإبرام العقود.

← قطر. وزارة المواصلات والاتصالات. قانون رقم ١٣ لسنة ٢٠١٦ بشأن حماية خصوصية البيانات الشخصية. <https://bit.ly/3vqhuf7>

• جمهورية مصر العربية:

قانون رقم ١٧٥ لسنة ٢٠١٨ في شأن مكافحة جرائم تقنية المعلومات):

صدر القانون عن وزارة الاتصالات وتكنولوجيا المعلومات، وكان الهدف من إصداره مكافحة جرائم تقنية المعلومات؛ والمقصود به أي وسيلة أو مجموعة وسائل مترابطة أو غير مترابطة تُستخدم لتخزين، واسترجاع، وترتيب، وتنظيم، ومعالجة، وتطوير، وتبادل المعلومات أو البيانات، ويشمل ذلك كل ما يرتبط بالوسيلة أو الوسائل المستخدمة سلكياً أو لاسلكياً، حيث أشار نص القانون وتحديداً في البند الثاني والثالث من المادة الثانية من القانون والتي تختص بالتزامات وواجبات مُقدم الخدمة حيث أوضحت نصاً "المحافظة على سرية البيانات التي تم حفظها وتخزينها، وعدم إفشائها أو الإفصاح عنها بغير أمر مسبب من إحدى الجهات القضائية المختصة، ويشمل ذلك البيانات الشخصية لأى من مستخدمي خدمته، أو أى بيانات أو معلومات متعلقة بالمواقع والحسابات الخاصة التي يدخل عليها هؤلاء المستخدمون، أو الأشخاص والجهات التي يتواصلون معها، وتأمين البيانات والمعلومات بما يحافظ على سريتها، وعدم اختراقها أو تلفها" ليصُد بعد ذلك قانون حماية البيانات الشخصية المصري والمتعلق بحماية البيانات الشخصية للأفراد من تعرضها للتعدي والانتهاك.

← جمهورية مصر العربية. وزارة الاتصالات وتكنولوجيا المعلومات. قانون رقم ١٧٥ لسنة ٢٠١٨ في شأن مكافحة جرائم تقنية المعلومات. <https://bit.ly/3b0pifa>

قانون حماية البيانات الشخصية المصري رقم ١٥١ لعام ٢٠٢٠):

تقدم مجلس النواب المصري بمشروع قانون حماية البيانات الشخصية في نوفمبر ٢٠١٧؛ والذي يعتبر الغرض منه ضمان وحماية كل ما يتعلق بمعالجة البيانات الشخصية للأفراد باعتبارها أحد أهم الحريات الشخصية والحقوق الأساسية للأشخاص الطبيعيين (الشامي، ٢٠١٧)

وفي المذكرة الإيضاحية تمت الإشارة إلى أهمية الحفاظ على خصوصية حياة المواطنين وعدم إفشاءها وحظر استخدام البيانات الشخصية للمواطنين إلا بموافقة أصحابها تطبيقاً لأحد مبادئ حقوق الإنسان العامة والتي نص عليها الدستور المصري في الفقرة الأولى من نص المادة (٥٧).

وفي أغسطس عام ٢٠١٨ وافق مجلس الوزراء المصري على مشروع قانون حماية البيانات الشخصية الذي يهدف إلى رفع مستويات أمن البيانات داخل الدولة، وتنظيم عمليات نقلها عبر الحدود

وأنشطة التسويق الإلكتروني (زكي، ٢٠١٨)، وتعتبر أبرز الأهداف وضع آليات كفيلة بالتصدي للأخطار الناجمة عن استخدام البيانات الشخصية للمواطنين ومكافحة انتهاك خصوصيتهم (أبو غزالة، ٢٠١٩)

وأكدت وزارة الاتصالات على أن قانون حماية البيانات الشخصية عنصر جذب للاستثمارات الأجنبية في مصر كإحدى وجهات الاستثمار الآمن؛ لما يتضمنه من حماية لخصوصية البيانات المتداولة عبر الدول والقارات. (عيد، ٢٠١٨)

وناقش مجلس النواب قانون حماية البيانات الشخصية في فبراير ٢٠٢٠ وأوضح أنه يهدف إلى التواكب مع اللائحة العامة لحماية البيانات الشخصية والخاصة بدول الاتحاد الأوروبي **GDPR** **General Data Protection Regulation**، وجاءت الموافقة على مشروع قانون حماية البيانات الشخصية واعتباره أحد مشروعات القوانين المكملة للدستور لا سيما مع خلو التشريعات المصرية من إطار قانوني ينظم حماية البيانات الشخصية المعالجة إلكترونياً أثناء جمعها وتخزينها أو معالجتها (فخري، ٢٠٢٠).

وبتاريخ ١٣/٧/٢٠٢٠ صدر القانون رقم ١٥١ لسنة ٢٠٢٠ والخاص بحماية البيانات الشخصية والذي عرف البيانات الشخصية بأنها " أي بيانات شخصية متعلقة بشخص طبيعي محدد، أو يمكن تحديده بشكل مباشر أو غير مباشر عن طريق الربط بين هذه البيانات وأي بيانات أخرى كالإسم، أو الصوت، أو الصورة، أو رقم تعريفى، أو محدد للهوية عبر الإنترنت أو أي بيانات تحدد للهوية النفسية، أو الصحية، أو الاقتصادية، أو الثقافية، أو الاجتماعية "

ويتكون القانون من ١٤ فصلاً ويتشكل من ٤٩ مادة، ويبدأ القانون بالفصل الأول الخاص بالتعريفات والتي أفرد لها شرح وافٍ للمعنى المبين لكل مصطلح يرد في هذا الشأن؛ وكما في القوانين السابقة أورد المشرع مصطلحات البيانات الشخصية، والبيانات الشخصية الحساسة، والمعالجة، ووضح مصطلحات كالشخص المعنى بالبيانات والحائز؛ فالمعنى بالبيانات هو أي شخص طبيعي تُنسب إليه بيانات شخصية معالجة إلكترونياً تدل عليه قانوناً أو فعلاً، وتُمكن من تمييزه عن غيره، والحائز هو أي شخص طبيعي أو اعتباري (مؤسسة أو هيئة أو مكتبة)؛ يحوز ويحتفظ قانونياً أو فعلياً ببيانات شخصية في أي صورة من الصور، أو على أي وسيلة تخزين سواء كان هو المُنشئ للبيانات، أم انتقلت إليه حيازتها بأي صورة.

كذلك تطرق لمصطلح التسويق الإلكتروني كما أشار له من قبل القانون القطري؛ حيث وضح المشرع أنه إرسال أي رسالة أو بيان أو محتوى إعلاني أو تسويقي بأي وسيلة تقنية الهدف منها الترويج لسلعة أو أو طلبات تجارية أو سياسية أو اجتماعية أو خيرية موجهة إلى اشخاص بعينهم؛ والإشارة إلى الطلبات الخيرية يوضح أن انتهاك خصوصية البيانات غير مشروط بالمكسب المادي أو التسويق في شكله التجاري فالانتهاك انتهاك أيا كانت الحالة. كما أضاف مصطلح الترخيص وهي وثيقة رسمية تصدر عن المركز للشخص الاعتباري تمنحه من خلالها الحق في مزاولة نشاط جمع البيانات الشخصية الإلكترونية أو تخزينها أو نقلها أو معالجتها أو القيام بأنشطة التسويق الإلكتروني والتعامل عليها بأي صورة.

ليأتي الفصل الثاني بعنوان حقوق المعنى بالبيانات وشروط جمع ومعالجة البيانات؛ ليوضح حقوق الشخص المعنى بالبيانات وهي كالتالي: العلم بالبيانات الشخصية الخاصة به؛ والموجودة لدى الحائز سواء كان شخص أو هيئة، والعدول عن الموافقة المسبقة؛ حيث يمكن الموافقة على إعطاء البيانات مع إعطاء الحق للعدول عن الموافقة وإيقافها، وحق التصحيح أو التعديل، أو المحو، أو الإضافة أو التحديث للبيانات الشخصية، والحق في العلم والمعرفة بأي خرق أو انتهاك لبياناته الشخصي، أيضاً الحق في الاعتراض على معالجة البيانات الشخصية أو نتاجها متى تعارضت مع الحقوق والحريات الأساسية للشخص المعنى بالبيانات؛ وما كان يمكن ممارسة البند الأخير من القانون في السابق؛ والخاص بالاعتراض بدون وجود قانون يضمن له الاعتراض؛ وتوضيح التعارض مع الحقوق والحريات الأساسية. ويأتي الفصل الثالث

ليوضح التزامات كل من المتحكم والمعالج من خلال القواعد المنظمة للعمل والمشار إليها بالفصل، مع توضيح شروط المعالجة؛ مع الالتزام بالإبلاغ في حالة العلم بوجود خرق أو انتهاك للبيانات الشخصية؛ ويتم ذلك في خلال ٧٢ ساعة. ويختص الفصل الرابع بمسؤولية حماية البيانات الشخصية من حيث تعيين المسؤول، والتزاماته من تنفيذ القانون ومراقبة الإجراءات. وتأتي إجراءات الإتاحة وماهية البيانات الحساسة في الفصلين الخامس والسادس، وما يهمنا عرضه هو الفصل التاسع والذي يُعنى بإنشاء مركز لحماية البيانات الشخصية؛ ويكون مسؤول عن وضع إطار إرشادي لتطبيق القرارات والضوابط والتدابير، والإجراءات والمعايير الخاصة بحماية البيانات الشخصية. وتختص باقي المواد بما يخص الضبطية القضائية والعقوبات المفروضة سواء كانت إدارية أو تصل للجرائم؛ وأوضحت المادة ٣٥ من القانون أن الغرامة في حالة العقوبات؛ لا تقل عن مائة ألف جنيه ولا تُجاوز مليون جنيه لكل حائز أو متحكم أو معالج جمع؛ عالج أو أفشى أو أتاح أو تداول بيانات شخصية معالجة إلكترونيًا بأي وسيلة من الوسائل في غير الأحوال المصرح بها قانونًا أو بدون موافقة الشخص المعني بالبيانات.

← جمهورية مصر العربية. وزارة الاتصالات وتكنولوجيا المعلومات. قانون حماية البيانات الشخصية المصري رقم ١٥١ لسنة ٢٠٢٠. <https://bit.ly/3N166fd>

• المملكة العربية السعودية (نظام حماية البيانات الشخصية رقم (م/١٩) لسنة ٢٠٢١):

تُشرف الهيئة السعودية للبيانات والذكاء الاصطناعي على تنفيذ هذا النظام أول عامين، وبعد ذلك، يتولّى "مكتب إدارة البيانات الوطنية" الإشراف على تنفيذه، تتوافق العديد من خصائص "نظام حماية البيانات الشخصية" السعودي مع المعايير والمبادئ الواردة في قوانين حماية البيانات الدولية الأخرى، مثل اللائحة العامة الأوروبية لحماية البيانات (GDPR) (2016/679)، أي اللائحة التي ينصّ عليها قانون الاتحاد الأوروبي حول حماية البيانات والخصوصية في الاتحاد الأوروبي والمنطقة الاقتصادية الأوروبية، والجدير بالذكر المادة الثالثة للقانون والتي تنص على إعطاء الأولوية للنظام القانوني الأكثر حماية للبيانات الشخصية (قرار قضائي، نظام قانوني آخر، معاهدة دولية تكون المملكة العربية السعودية طرفًا فيها)، كذلك أكد نص القانون في المادة الثانية عشر على أنه وفقًا لنظام حماية البيانات الشخصية، على جهة التحكّم أن تعتمد سياسة للخصوصية، وأن تجعلها متاحة للمعنيين ليطلعوا عليها قبل جمع بياناتهم الشخصية، ويحدّد النظام الحد الأدنى من المعلومات التي يجب إدراجها في سياسة الخصوصية، بما في ذلك الحالات التي يتمّ فيها جمع البيانات الشخصية مباشرةً من صاحب البيانات.

← المملكة العربية السعودية. الهيئة السعودية للبيانات والذكاء الاصطناعي. نظام حماية البيانات الشخصية رقم (م/١٩) لسنة ٢٠٢١. <https://bit.ly/3xZbY4a>

- وتجدر الإشارة إلى اتفاق تشريعات وقوانين حماية الخصوصية في الدول العربية في لائحته التنفيذية فيما يخص الحق في التعديل والحذف والإضافة من خلال تقديم طلب رسمي للجهات المعنية مُحدد المُدة.

- واختلفت تشريعات وقوانين الخصوصية للدول العربية فيما بينها في مسؤولية الجهات المُصدرة لهذه القوانين؛ حيث انحصرت في خمسة جهات مُصدرة للقوانين وهي: وزارة العدل، ووزارة الاتصالات وتكنولوجيا المعلومات، والهيئة السعودية للبيانات والذكاء الاصطناعي، وحكومة دبي، وديوان التشريع والرأي الأردني، كما يوضح الجدول رقم (٣-١).

جدول رقم (١-١) قوانين حماية البيانات الشخصية بالدول العربية

م	الدولة	اسم القانون	الجهة المسؤولة عن إصدار القانون	سنة إصدار القانون
١	تونس	قانون رقم ٦٣ لسنة ٢٠٠٤ والمتعلق بحماية المُعطيات الشخصية	وزارة العدل	٢٠٠٤
٢	المملكة المغربية	قانون رقم ٠٩،٠٨ لسنة ٢٠٠٩ والمتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي	وزارة العدل	٢٠٠٩
٣	المملكة الأردنية الهاشمية	مشروع قانون حماية البيانات الشخصية لسنة ٢٠١٤	وزارة الاتصالات الأردنية	٢٠١٤
٤	إمارة دبي	مبادرة بيانات دبي	حكومة دبي	٢٠١٥
٥	الإمارات العربية المتحدة	القانون الاتحادي رقم ١٢ لسنة ٢٠١٦ لحماية البيانات والخصوصية	وزارة العدل	٢٠١٦
٦	قطر	قانون رقم ١٣ لسنة ٢٠١٦ بشأن حماية خصوصية البيانات الشخصية	وزارة المواصلات والاتصالات	٢٠١٦
٧	جمهورية مصر العربية	قانون رقم ١٧٥ لسنة ٢٠١٨ في شأن مكافحة جرائم تقنية المعلومات	وزارة الاتصالات وتكنولوجيا المعلومات	٢٠١٨
٨	جمهورية مصر العربية	قانون حماية البيانات الشخصية المصري رقم ١٥١ لسنة ٢٠٢٠	وزارة الاتصالات وتكنولوجيا المعلومات	٢٠٢٠
٩	المملكة الأردنية الهاشمية	قانون حماية البيانات الشخصية لسنة ٢٠٢٠	ديوان التشريع والرأي	٢٠٢٠
١٠	المملكة العربية السعودية	نظام حماية البيانات الشخصية رقم (١٩/م) لسنة ٢٠٢١	الهيئة السعودية للبيانات والذكاء الاصطناعي	٢٠٢١

٢/١ قوانين حماية خصوصية البيانات عالمياً:

تعرض الدراسة للقوانين والتشريعات العالمية، المعنية بحماية خصوصية بيانات الأفراد؛ بداية من الولايات المتحدة الأمريكية؛ مع الإشارة لقانون باتريوت الأمريكي لمكافحة الإرهاب، ولائحة الاتحاد الأوروبي العامة لحماية البيانات.

الولايات المتحدة الأمريكية:

تفتقر الولايات المتحدة إلى قانون فيدرالي موحد يهدف إلى حماية البيانات الشخصية للأفراد ويُجنبها محاولات الانتهاك والاختراق؛ لذلك يجب البدء بمقدمة تاريخية توضح توجه الولايات المتحدة الأمريكية ونظرتها لقوانين حماية البيانات الشخصية من خلال عرض لبعض القوانين المنظمة للبيانات ومنها قانون

الخصوصية الأمريكية الفيدرالي لعام ١٩٧٤ ، وقانون باتريوت لسنة ٢٠٠١ **USA PATRIOT Act** ، وقانون حماية خصوصية المستهلك في كاليفورنيا **California Consumer Privacy Act 2020** .CCPA

قانون الخصوصية الأمريكي الفيدرالي لعام ١٩٧٤ :

يضع قانون الخصوصية الأمريكي الفيدرالي لعام ١٩٧٤ قيودًا على جمع المعلومات الشخصية واستخدامها ونشرها من قبل الحكومة الفيدرالية. ويمكن إرجاع أصل قانون الخصوصية إلى عام ١٩٦٥ عندما قامت لجنة فرعية تابعة للكونجرس الأمريكي بفحص قضايا الخصوصية وأصدرت عدد من التقارير حول تأثير حقوق الخصوصية الفردية بنمو بنوك البيانات الوطنية وتطور حركة جمع البيانات الإلكترونية وتخزينها. وكان أحد العوامل المحفزة للتشريع هو تقرير وزارات الصحة والتعليم والرعاية الاجتماعية عن السجلات الحكومية وأجهزة الكمبيوتر. واقترح التقرير مدونة بعنوان: ممارسات المعلومات العادلة تشمل خمسة مبادئ أساسية هي:

- ١- يجب على الحكومة ألا تحتفظ بأي سجلات سرية.
- ٢- يجب أن يكون الأفراد قادرين على رؤية المعلومات الشخصية الخاصة بهم المخزنة وكيفية استخدامها.
- ٣- يجب على الأفراد تقديم موافقة كتابية مسبقة قبل أن يتم استخدام المعلومات الشخصية التي تم جمعها عنهم.
- ٤- يجب السماح للأفراد بإصلاح أو توضيح المعلومات الشخصية عنهم.
- ٥- يجب أن تكون المنظمات التي تخزن أو تستخدم البيانات الشخصية مسؤولة عن صحة المعلومات ويجب منع إساءة استخدامها.

→USA. The federal government. The Privacy Act of 1974.

<https://bit.ly/3xYLIXL>

قانون باتريوت الأمريكي لمكافحة الإرهاب 2001 USA PATRIOT Act :

هو قانون صادر عن الكونجرس الأمريكي تحت ولاية الرئيس الأمريكي الأسبق جورج. و. بوش أقر بعد أحداث ١١ سبتمبر ٢٠٠١، وهو خاص بتسهيل إجراءات التحقيقات و الوسائل اللازمة لمكافحة الإرهاب، مثل إعطاء أجهزة الشرطة صلاحيات من شأنها الاطلاع على المقتنيات الشخصية للأفراد و مراقبة اتصالاتهم و التنصت على مكالماتهم بغرض الكشف عن المؤامرات الإرهابية.

هذا القانون يعطي الهيئات التنفيذية المتمثلة في أجهزة الشرطة و مكتب التحقيقات الفيدرالي صلاحيات واسعة في مجال مراقبة و تفتيش المشتبه فيهم دون أن يكون لديهم أدلة ملموسة تدينهم بشكل مباشر ودون فرض رقابة كافية على تلك الصلاحيات، ماعدا فقط اعطاء القضاء الأمريكي صلاحية مراقبة عمل أجهزة الشرطة مع عدم تبني مزيد من التدابير التي تدعم هذه الصلاحية ، مثل إنشاء وكالة مستقلة للحريات المدنية تعمل على مراقبة FBI.

→USA. Act of Congress. USA PATRIOT Act of 2001. <https://bit.ly/3vT5nHz>

وهو ما تستخدمه الولايات المتحدة الأمريكية كحجة لحماية الأمن القومي الأمريكي من خلال التجسس على المواطنين وصولاً إلى التجسس على تطبيقات الهاتف المحمول من خلال بعض منصات وسائل التواصل الاجتماعي مثل فيسبوك Facebook فيما عُرف باسم " فضيحة كامبريدج أناليتيكا " والتي اتهمت على أثرها شركة فيسبوك بانتهاك خصوصية مستخدميها من خلال السماح لشركة كامبريدج

أناليتيكا بالحصول على بيانات عشرات الملايين من المستخدمين، وفي بريطانيا، فرضت السلطات غرامة على فيسبوك بقيمة ٥٠٠ مليون جنيه استرليني، بسبب تورطها في فضيحة كامبريدج أناليتيكا، وهي أقصى غرامة يمكن أن تفرضها هيئة تنظيم البيانات في المملكة المتحدة، مما يُهدد الخصوصية ويُعد انتهاكًا للحريات؛ حيث يتم الاطلاع غير المشروع على بيانات المستخدمين والربط فيما بينها واستخدامها في التسويق لمنتجات معينة، أو التأثير على رغبات الشراء والاقتناء بناءً على معلومات مُسبقة عن سلوك المُستخدمين من خلال تتبع عمليات البحث التي يقوم بها المستخدم على هذه المنصات. (فضيحة كامبريدج أناليتيكا، ٢٠١٨)

قانون حماية خصوصية المستهلك في كاليفورنيا 2020 California Consumer Privacy Act :CCPA

يمنح قانون خصوصية المستهلك في كاليفورنيا لعام ٢٠١٨ (CCPA) للمستهلكين مزيدًا من التحكم في المعلومات الشخصية التي تجمعها الشركات عنهم وتوفر لوائح CCPA إرشادات حول كيفية تنفيذ القانون، ويضمن هذا القانون التاريخي حقوق الخصوصية الجديدة للمستهلكين في كاليفورنيا، بما في ذلك:

الحق في معرفة المعلومات الشخصية التي تجمعها الشركة عنهم وكيفية استخدامها ومشاركتها.

الحق في حذف المعلومات الشخصية التي تم جمعها منهم.

الحق في إلغاء الاشتراك في بيع معلوماتهم الشخصية؛ والحق في عدم التمييز بسبب ممارسة حقوقهم في قانون حماية خصوصية المستهلك في كاليفورنيا.

كما يتعين على الشركات إعطاء المستهلكين إخطارات معينة تشرح ممارسات الخصوصية الخاصة بهم.

وهو ما يمكن تطبيقه في سياسات المكتبات الأكاديمية من حيث الإبلاغ الكامل عن البيانات المُحتفظ بها للمستخدمين داخل المكتبة، مع إعطاء الحق كاملاً في التعديل والحذف والإضافة على هذه البيانات وفي أي وقت بعد التقدم بطلب لذلك وانتظار الوقت المتفق عليه لإنفاذ الطلب؛ مع التعهد بالحفاظ على سرية وخصوصية البيانات المُحتفظ عليها لدى المكتبة؛ والحفاظ عليها من الانتهاك أو الإفشاء غير المُصرح به.

→USA. State of California Department of Justice. California Consumer Privacy Act (CCPA). <https://bit.ly/3FoEnTe>.

لائحة الاتحاد الأوروبي العامة لحماية البيانات

GDPR General Data Protection Regulation

جاءت لائحة الاتحاد الأوروبي العامة لحماية البيانات GDPR General Data Protection Regulation في ٩٩ مادة مقسمة على ١١ فصل؛ حيث يبدأ الفصل الأول بمجموعة من الأحكام العامة والتي تشمل الأهداف، ونطاق تطبيق القانون إقليميًا، ويوضح بأنه لا يمكن تطبيق هذا القانون في معالجة البيانات الشخصية في بعض الحالات وهي: في سياق نشاط يقع خارج نطاق قانون الاتحاد؛ من قبل الدول الأعضاء عند القيام بأنشطة تقع ضمن نطاق تطبيق القانون؛ من قبل شخص طبيعي في سياق نشاط شخصي أو منزلي بحت؛ من جانب السلطات المختصة لأغراض منع الجرائم الجنائية أو التحقيق فيها أو اكتشافها أو مقاضاة مرتكبيها أو تنفيذ العقوبات الجنائية، بما في ذلك صون ومنع التهديدات التي يتعرض لها الأمن العام.

ويتناول الفصل الثاني المبادئ المتعلقة بمعالجة البيانات الشخصية ومن أهمها: أن تكون " جُمعت لأغراض محددة وصریحة ومشروعة ولم تتم معالجتها بطريقة تتنافى مع هذه الأغراض؛ ولا تعتبر

المعالجة الإضافية لأغراض الأرشفة للمصلحة العامة أو لأغراض البحث العلمي أو البحثي أو الأغراض الإحصائية" وهو ما يُقصد به تحديد الهدف عند الشروع في إعداد سياسة لحماية خصوصية البيانات الشخصية للمستفيدين في المؤسسات ولا سيما المكتبات الأكاديمية؛ لحساسية التعامل في معالجة البيانات الشخصية، وإعطاء موثوقية أكثر عند التعامل مع المكتبة.

ووضعت المادة السابعة من القانون شرط الموافقة على معالجة البيانات وأوضحت أن الموافقة يجب أن تكون واضحة ومثبتة على أن صاحب البيانات وافق بالفعل على السماح بمعالجة بياناته.

ليبدأ الفصل الثالث بحقوق صاحب البيانات وتشترط المادة ١٢ من القانون أن تعرض حقوق صاحب البيانات بطريقة واضحة وبلغة سهلة على الفهم وبمفردات سلسة توضح له حقوقه، والإجراءات المتخذة لتغيير البيانات، وأن يتم ذلك في خلال شهر من التقدم بالطلب ولا يزيد عن تلك الفترة.

وتأتي المادة ١٥ لتوضح بند غاية في الأهمية وهو حق الوصول عن طريق صاحب البيانات؛ حيث يحق لصاحب البيانات الحصول على تأكيد من وحدة معالجة البيانات المعنية بمعالجة بياناته - كالمكتبة الأكاديمية التابع لها المستفيد - ما إذا كانت بياناته يتم معالجتها أم لا؛ ويحق له الحصول على البيانات التالية:

١. أغراض المعالجة.
٢. فئات البيانات المعنية.
٣. المستلمون أو فئات المستلمين الذين تم الكشف عن بياناتهم الشخصية أو سيتم الكشف عنها، ولا سيما المستلمون في بلدان ثالثة أو المنظمات الدولية.
٤. الفترة الزمنية التي ستخزن فيها البيانات الشخصية، أو، إن لم يكن ممكناً، المعايير المستخدمة لتحديد تلك الفترة.
٥. وجود حق له تجاه المراقب لطلب أو تصحيح أو محو البيانات الشخصية أو تقييد معالجة البيانات الشخصية المتعلقة بصاحب البيانات أو الاعتراض عليها.
٦. الحق في تقديم شكوى لدى سلطة إشرافية.

وتأتي المادة ١٧ لتوضح الحق في المحو (الحق في النسيان) **The right to be forgotten** حيث يحق لصاحب البيانات أن يحصل من المراقب على حق محو البيانات الشخصية المتعلقة به دون تأخير لا مبرر له، و يجب أن يتحمل المتحكم مسئولية محو البيانات الشخصية دون أي تأخير لا مبرر له.

وأقرت اللائحة موضوع أمن البيانات الشخصية في المادة ٣٢ من القانون؛ حيث راعت أحدث ما توصلت إليه التكنولوجيا، وتكاليف التنفيذ، وطبيعة المعالجة، ونطاقها، وسياقها، وأغراضها، فضلاً عن مخاطر تنوع الاحتمالات وشدتها بالنسبة لحقوق وحرية الأشخاص الطبيعيين ووحدة التحكم والمعالج، ويجب تنفيذ التدابير التقنية والتنظيمية المناسبة لضمان مستوى من الأمن مناسب للمخاطر كالأسم المستعار وتشفير البيانات الشخصية، والقدرة على استعادة التوافر والوصول إلى البيانات الشخصية في الوقت المناسب في حالة وقوع حادث مادي أو تقني، وعملية الاختبار والتقييم وتقييم فعالية الإجراءات التقنية والتنظيمية لضمان أمن المعالجة.

وأقرت اللائحة في المادة ٨٢ الحق في التعويض والمسؤولية؛ حيث يحق لأي شخص عانى من ضرر مادي أو غير مادي نتيجة لانتهاك هذه اللائحة الحصول على تعويض من المراقب أو المعالج عن الأضرار التي لحقت به مع تحمل أي وحدة تحكم تشارك في المعالجة المسؤولية عن الأضرار الناجمة عن المعالجة التي تنتهك هذه اللائحة. ويكون المعالج مسؤول عن الضرر الناجم عن المعالجة فقط في الحالات

التي لا يمتثل فيها للالتزامات هذه اللائحة الموجهة تحديداً إلى المعالجات أو حيث يكون قد تصرف خارج نطاق أو مخالفاً للتعليمات القانونية لجهاز التحكم.

وتختص المادة ٨٤ بالجزاءات حيث تضع الدول الأعضاء القواعد المتعلقة بالعقوبات الأخرى السارية على مخالفات هذه اللائحة، لا سيما فيما يتعلق بالانتهاكات التي لا تخضع للغرامات الإدارية بموجب المادة ٨٣ ، وتتخذ جميع التدابير اللازمة لضمان تنفيذها. وتكون هذه العقوبات فعالة ومتناسبة وراذعة.

→The European Union. General Data Protection Regulation GDPR.
<https://bit.ly/3FuM2Qe>.

٣/١ مقارنة بين قانون حماية البيانات الشخصية المصري رقم ١٥١ لعام ٢٠٢٠ واللائحة العامة لحماية البيانات الشخصية GDPR General Data Protection Regulation والصادرة عن الاتحاد الأوروبي:

تطرح الدراسة تساؤلاً حول أهمية التوافق بين القوانين المحلية ومنها القانون المصري لحماية البيانات الشخصية وما بين القوانين العالمية كاللائحة العامة لحماية البيانات الشخصية GDPR والخاصة بئول الاتحاد الأوروبي، حيث تجدر الإشارة إلى أن تطورات تكنولوجيا المعلومات والاتصالات المتلاحقة، وخاصة مع بزوغ تكنولوجيا الذكاء الاصطناعي والحوسبة السحابية؛ أدت إلى ظهور تحديات جديدة على مستوى حماية البيانات الشخصية، حيث زاد نطاق وحجم جمع وتبادل ومعالجة هذه البيانات إلكترونياً بشكل كبير، مما سمح للشركات والمؤسسات الخاصة والعامة باستخدام البيانات الشخصية للأفراد على نطاق واسع نظراً لأن الأنشطة الإلكترونية القائمة على جمع وتحليل واستنباط وتخزين تلك البيانات تساعد الشركات والمؤسسات على الاستفادة الاقتصادية والتجارية من تلك البيانات الرقمية بشكل متزايد (دراسة نقدية حول قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠، ٢٠٢٠) وعليه أصبحت التعاقبات بين الدول فيما يخص عمليات نقل ومعالجة البيانات تتم بكل سهولة من خلال خوادم عملاقة يتحكم بها ويديرها طرف ثالث يقف بين مقدمي الخدمات وما بين المستفيدين، ولهذا شكّل التوافق بين قوانين تنظيم البيانات بين الدول أهمية كبرى وأثر بشكل كبير على تحديد بنود في العقود تؤمن عمليات نقل وتخزين البيانات؛ بما يحفظ خصوصيتها ويحميها من الانتهاكات والخروقات الأمنية.

جاء مشروع حماية البيانات الشخصية المصري رقم ١٥١ لعام ٢٠٢٠ متوخياً الأهداف التالية:

- ضمان مستوى مناسب من الحماية القانونية والتقنية للبيانات الشخصية المُعالجة إلكترونياً.
- وضع آليات كفيلة بالتصدي للأخطار الناجمة عن استخدام البيانات الشخصية للمواطنين، ومكافحة انتهاك خصوصيتهم.
- تطبيق إطار معياري يتواءم مع التشريعات الدولية لحماية البيانات الشخصية للأفراد، وحيرياتهم، واحترام خصوصيتهم.
- صياغة التزامات على كل من المتحكم في البيانات، ومعالج البيانات باعتبارهما من العناصر الفاعلة في مجالات التعامل في البيانات الشخصية، سواء عن طريق الجمع أو النقل أو التبادل أو التخزين أو التحليل أو المعالجة بأي صورة من الصور.
- إلزام المؤسسات والجهات والأفراد المتحكمين في البيانات الشخصية، والمعالجين لها بتعيين مسئول لحماية البيانات الشخصية داخل مؤسساتهم وجهاتهم، بما يسمح بضمان خصوصية بيانات الأفراد، واقتضاء حقوقهم المنصوص عليها في هذا القانون.

- تقنين وتنظيم أنشطة استخدام البيانات الشخصية في عمليات الإعلان والتسويق على الإنترنت، وفي البيئة الرقمية بشكل عام.
- وضع إطار إجرائي لتنظيم عمليات نقل البيانات عبر الحدود وضمان حماية بيانات المواطنين وعدم نقلها أو مشاركتها مع دول لا تتمتع بالبيانات بالحماية.
- تنظيم العمليات المعالجة إلكترونيًا للبيانات الشخصية، وإصدار تراخيص لمن يقوم بها، وعلى الأخص فيما يتعلق بالبيانات الشخصية الحساسة.
- إنشاء مركز حماية البيانات الشخصية كهيئة عامة يكون مختصًا بتنظيم والإشراف على تنفيذ أحكام القانون. (وزارة الاتصالات وتكنولوجيا المعلومات. تقرير اللجنة المشتركة من لجنة الاتصالات وتكنولوجيا المعلومات ومكاتب لجان الشئون الدستورية والتشريعية، الخطة والموازنة والدفاع والأمن القومي، ٢٠١٩)

وفيما يلي مقارنة لبعض أوجه الاختلاف والاتفاق بين قانون حماية البيانات الشخصية المصري رقم ١٥١ لعام ٢٠٢٠، واللائحة العامة لحماية البيانات الشخصية والصادرة عن الاتحاد الأوروبي، كما يوضح الجدول رقم (٢-١).

جدول رقم (٢-١) مقارنة بين قانون حماية البيانات الشخصية المصري رقم ١٥١ لعام ٢٠٢٠ واللائحة العامة لحماية البيانات الشخصية والصادرة عن الاتحاد الأوروبي

وجه المقارنة	قانون حماية البيانات الشخصية المصري رقم ١٥١ لعام ٢٠٢٠	اللائحة العامة لحماية البيانات الشخصية والصادرة عن الاتحاد الأوروبي
الإطار المفاهيمي	اقتصرت التعريف على البيانات المتعلقة بالأشخاص الطبيعيين فقط	توسع بعض الشيء في بيان المسائل الخاصة التي يمكن الاستعانة بها لتحديد هوية الشخص الطبيعي مثل المعلومات الجينية أو العقلية
حقوق الشخص المعني بالبيانات	<ul style="list-style-type: none"> - حق العلم بالبيانات الشخصية والإطلاع عليها والوصول إليها أو الحصول عليها. - حق العدول عن الموافقة على الاحتفاظ بالبيانات أو معالجتها. - الحق في تصحيح أو تعديل أو محو البيانات الشخصية. 	<ul style="list-style-type: none"> - الحق في الوصول للبيانات Right of Access. - الحق في سحب الموافقة The right to withdraw of consent. - الحق في التصحيح Right to rectification، والحق في المحو Right to be forgotten.
شروط معالجة البيانات	<ul style="list-style-type: none"> - الحصول على البيانات الشخصية أو تلقيها من الحائز أو من الجهات المختصة بتزويده بها بحسب الأحوال بعد موافقة الشخص المعني بالبيانات، أو في الأحوال المصرح بها قانوناً. - التأكد من صحة البيانات الشخصية واتفاقها وكفايتها مع الغرض المحدد لجمعها. - وضع طريقة وأسلوب ومعايير المعالجة 	<ul style="list-style-type: none"> - وضع المشرع الأوروبي نفس الالتزام باللائحة. - قررت اللائحة الأوروبية التزاماً على عاتق المتحكم بتنفيذ التدابير الفنية والتنظيمية المناسبة لضمان معالجة البيانات لغرض محدد. - تتفق اللائحة الأوروبية في ذلك مع القانون المصري.

وجه المقارنة	قانون حماية البيانات الشخصية المصري رقم ١٥١ لعام ٢٠٢٠	اللائحة العامة لحماية البيانات الشخصية والصادرة عن الاتحاد الأوروبي
	<ul style="list-style-type: none"> طبقاً للغرض المحدد. محو البيانات الشخصية فور انقضاء الغرض المحدد منها. تحديد من سيفصح أو يتيح هذه البيانات، وسنده والمدد الزمنية وقيودها ونطاقها وآليات محو أو تعديل البيانات الشخصية لدى الجهة. 	<ul style="list-style-type: none"> حق الأفراد في مسح ومحو البيانات الشخصية. يتسق مسلك المشرع الأوروبي مع المشرع المصري.
وسائل إنفاذ القانون	<ul style="list-style-type: none"> إنشاء مركز حماية البيانات الشخصية للإشراف على تطبيق هذه القوانين. 	<ul style="list-style-type: none"> إنشاء هيئات ومراكز تُشرف على تطبيق القوانين.

وتجدر الإشارة إلى أنه لا توجد ضرورة لتطابق القانون المصري بصورة كاملة مع اللائحة الأوروبية لحماية البيانات الشخصية وذلك لوجود اختلافات عديدة بين كل من النظامين القانونيين في شأن تطور التشريعات المنظمة لحماية البيانات الشخصية. (دراسة نقدية حول قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠، ٢٠٢٠)

٤/١ نماذج لسياسات حماية خصوصية بيانات المُستفيدين بالمكتبات الأكاديمية عربياً وعالمياً:

اهتمت الدراسة بعرض نماذج لسياسات الخصوصية للمكتبات الأكاديمية عربياً وعالمياً؛ للتعرف على محتويات السياسات، واهتمت باستعراض سياسات خصوصية البيانات في المكتبات الأكاديمية بالدول التي لها تشريعات تختص بحماية البيانات، وتلك التي ليست لديها تشريعات بعد.

١/٤/٣ سياسات حماية خصوصية بيانات المُستفيدين بالمكتبات الأكاديمية عربياً:

■ المملكة العربية السعودية:

جاءت سياسات المكتبات في المملكة العربية السعودية على النحو التالي:

- **السياسة العامة لمكتبات جامعة الجوف:** جاء ذكر الخصوصية مصاحباً لتأمين البيانات كعنصر من عناصر السياسة العامة للمكتبة، كالتالي: "تحقيق مبدأ الأمن المعلوماتي، خصوصاً ما ورد في حفظ حقوق الملكية للمؤلفين، وأيضاً الحفاظ على خصوصية مستفيدي المكتبات". (مكتبات جامعة الجوف. السياسة العامة، ٢٠٢١).

- **سياسات الخصوصية لجامعة الملك فيصل:** لا توجد سياسة خاصة بالمكتبات الجامعية؛ وإنما سياسة عامة للجامعة بشكل عام، أوضحت السياسة الإجراءات التي تتخذها الجامعة في الحفاظ على أمن المعلومات وخصوصية بيانات الطلبة؛ وما يميز هذه السياسة هو وضع بعض الضوابط والإجراءات المُساعدة في الحفاظ على خصوصية منسوبيها وجاءت على النحو التالي: "لكي تتمكن عمادة التعلم الإلكتروني والتعليم عن بُعد من مساعدة المستخدم في حماية معلوماته الشخصية، فإن العمادة توصي المستخدم بما يلي: الاتصال بالدعم الفني بشكل فوري عندما يغلب على ظن المستخدم أن شخصاً ما استطاع الحصول على كلمة السر الخاصة به، أو رمز الاستخدام، أو الرقم السري، أو أي معلومات سرية أخرى، عدم الإفصاح عن أي معلومات سرية عبر الهاتف أو شبكة الإنترنت ما لم تعرف هوية الشخص أو الطرف المستقبل للمعلومة،

استخدام متصفحات آمنة عند القيام بإنجاز المعاملات عبر الإنترنت، مع إغلاق التطبيقات غير المستخدمة على الشبكة، والتأكد من أن برنامج الحماية من الفيروسات محدثة على الدوام (سياسة الأمن السيبراني، ٢٠٢١)، و في حالة وجود أية استفسارات أو آراء حول وثيقة الخصوصية وما تحويه من مبادئ، يمكن التواصل مع إدارة البوابة عبر البريد الإلكتروني بالموقع، وللحفاظ على البيانات الشخصية، يتم تأمين التخزين الإلكتروني والبيانات الشخصية المرسله باستخدام التقنيات الأمنية المناسبة". (جامعة الملك فيصل. سياسة الخصوصية، ٢٠٢٠)

■ سلطنة عُمان:

- سياسة خصوصية جامعة السلطان قابوس: جاء ذكر الخصوصية في الجزء الخاص بضوابط السلوك بلوائح المكتبة المركزية للجامعة، وُجّهت التعليمات لمُقدمي خدمات المعلومات على النحو التالي: " لا يجوز للموظف الكشف عن أي معلومات سرية تخص المكتبة لأي شخص مهما كانت الظروف، إلا في نطاق واجباتهم وحدود صلاحياتهم، كما لا يجوز الوصول إلى حسابات المستفيد باستثناء المستفيد الموجود أمامه، أو الموجود على خط الهاتف، كما يجب التقيد بحفظ وحماية ورفع الوعي بضرورة الالتزام بحقوق الملكية الفكرية الواردة في قانون حقوق المؤلف والحقوق المجاورة العماني". (جامعة السلطان قابوس. ضوابط السلوك، ٢٠٢٢)

■ دولة قطر:

- سياسة خصوصية مكتبة قطر الرقمية: في البداية توضح السياسة أن المكتبة تجمع عدد من المعلومات تخص المُستفيد وهي: الأسئلة، والاستفسارات أو الملاحظات التي يتركها، بما في ذلك عنوان البريد الإلكتروني، وعنوان بروتوكول الإنترنت للجهاز الذي استخدمه، وتفاصيل نوع إصدار متصفح الويب الذي استخدمته وغيرها من المعلومات التقنية عن الجهاز؛ وأوضحت السياسة أن الغرض من تجميع المعلومات هو تحسين الموقع من خلال معرفة كيفية استخدامه، والرد على أي ملاحظات أو تعليقات أو استفسارات مُرسلة، كما توضح السياسة التزام مكتبة قطر الرقمية بالتحكم في خصوصية بياناتها فقط وتوضح بأنها غير ملتزمة مع المُستفيد بأية التزامات تجاه المواقع الأخرى التي قد تستخدم المكتبة روابط تُقود إليها، وتوضح أن تخزين البيانات يتم على خوادم آمنة؛ ولا يطلّع عليها سوى موظفي مكتبة قطر الرقمية المختصين أو مصمميها، وتوضح السياسة فيما يخص تخزين البيانات أن "تُخزّن المكتبة أكبر قدر ممكن من بياناتك كتفاصيل ومعلومات غير محددة الهوية، ولن نستخدم أبدًا هذه المعلومات في تحديد هوية مستخدمين بعينهم أو لربطها ببيانات أخرى حول مستخدم بعينه. كما لن نتبادل بياناتك مع أي مؤسسات أو شركات أخرى لأغراض تسويقية أو تجارية أو بحثية عن السوق، ولن ننقل بياناتك لأي مواقع أخرى على الإنترنت". (مكتبة قطر الرقمية. سياسة الخصوصية، ٢٠١٧)

■ لبنان:

- سياسات الخصوصية لمكتبات الجامعة الأمريكية في بيروت AUB Library: أوضحت المكتبة في بداية سياستها اتفاقها مع وثيقة ALA حول الخصوصية في المكتبات، وبيان الإفلا IFLA حول المكتبات والحرية الفكرية، كذلك أوضحت أنها تتفق القوانين والتشريعات اللبنانية المتعلقة بالخصوصية، وتتنطبق هذه السياسة على جميع موارد المكتبات وخدماتها، بغض النظر عن شكلها ووسائل إيصالها، وأوضحت السياسة بأن طلبات الإفصاح الرسمية عن أية بيانات أو معلومات عن المُستفيدين تختص بالرد عليها إدارة الشؤون القانونية بالجامعة الأمريكية ببيروت، وقُسمت السياسة وفقًا للخدمات المُقدمة إلى:

- **خدمات الاستعارة:** لن يكشف الموظفون عن أسماء الأفراد المستعيرين أو تاريخ استعارتهم للكتب.
- **تتمة المُقتنيات:** تعتبر أوامر الشراء المرتبطة بالمستخدمين سرية ولا ينبغي مشاركتها مع أشخاص خارج نطاق العمل.
- **خدمات الفهرسة ووصف البيانات:** تُعتبر عمليات استعجال معالجة كتاب مُعين أو معاملته كأولوية سرية لا يجب الإفصاح عنها.
- **العقود والتراخيص:** يجب أن تحمي العقود والتراخيص والاتفاقيات التي تبرمها المكتبات مع المستخدمين والموردين والمؤسسات الزميلة هوية المستخدمين الأفراد والمعلومات التي يستخدمونها، كما يجب الحفاظ على هذه الاتفاقيات في مكان آمن ويجب عدم مشاركتها مع أشخاص خارج نطاق العمل.
- **خدمات المصادر الإلكترونية:** قد يتم تجميع المعلومات والبيانات التي تم الحصول عليها من استخدام المصادر الإلكترونية، مثل أجهزة الكمبيوتر وقواعد البيانات والإنترنت لإعداد التقارير عن استخدام المواد وسيتم تخزينها لفترة زمنية معينة، وستبقى المعلومات سرية ولن يتم مشاركتها مع أطراف أخرى.
- **خدمات الإعارة بين المكتبات وخدمات توصيل الوثائق:** طلبات الإعارة بين المكتبات وخدمات تسليم الوثائق سرية، فلا يجب على مُقدمي الخدمة تضمين اسم المستفيد في الطلب المقدم إلى المكتبة ما لم يكن ذلك ضرورياً؛ وإذا كانت هناك حاجة إلى معلومات تعريف فردية، فيجب أخذ أرقام التعريف بدلاً من أسماء المستخدمين للحفاظ على السرية، ويجب الاحتفاظ بملفات جميع الطلبات المعبأة للعام الحالي والسنوات التقويمية الثلاثة الماضية للائتمثال للتدقيق والأرشفة واللوائح الأخرى.
- **استبانات المكتبة:** تعتبر المعلومات الخاصة التي تجمعها المكتبات بناءً على استطلاع أو تقييم الخدمة سرية ولن يتم الكشف عنها لأطراف أخرى أو استخدامها خارج نطاق المسح.
- **الخدمات المرجعية:** تُعتبر أية معلومات تتعلق بهوية مستفيدي المكتبة، وطبيعة وموضوع استفسارهم، والموارد التي استخدموها مع أمين المكتبة سرية. (AUB. USERS' **PRIVACY AND CONFIDENTIALITY**، 2016)

■ فلسطين:

- **سياسة الخصوصية لمكتبة جامعة القدس المفتوحة:** حيث توضح السياسة أنها الجامعة تلتزم بحماية خصوصية مستفيديها فيما يخص المعلومات الشخصية التي تجمعها جامعة القدس المفتوحة عبر مواقعها الإلكترونية (موقع الجامعة، البوابة الأكاديمية، البوابة الإدارية، بوابة خريجو الجامعة، بوابة المكتبة، موقع مركز التعليم المستمر وخدمة المجتمع) ولا تنطبق على المعلومات التي تجمعها الجامعة بأي أسلوب آخر؛ وركزت السياسة على عنصرين، الأول **يختص بجمع وحفظ المعلومات:** وجاء فيها "أن الجامعة قد تطلب منك أن تقدم معلومات شخصية، منها، اسمك، وعنوانك، وبريدك الإلكتروني، ورقم هاتفك، ورقم البطاقة الشخصية الخاصة بك، ومعلومات الاتصال، وأية معلومات أخرى تحدد من خلالها هويتك الخاصة. وفي أقسام أخرى من الموقع قد تجمع جامعة القدس المفتوحة معلومات ديموجرافية ليست منفردة بك مثل الدولة التي تقيم بها، والعمر، والمستوى التعليمي، والجنس، وغيرها من أنواع المعلومات المشابهة، وأحياناً تجمع

جامعة القدس المفتوحة مزيجًا من هذين النوعين من المعلومات" وتوضح أسباب طلب المعلومات من أجل جعل زيارتك المتكررة للموقع أكثر فعالية وتخصصًا وكذلك من أجل المحافظة على معلوماتك بأسلوب فعال، فإن جامعة القدس المفتوحة تحفظ المعلومات التي تجمعها، **والعنصر الثاني يختص بالتصفح:** حيث توضح السياسة الغرض من جمع المعلومات كالتالي "قد تقوم خوادم الويب التابعة لنا بجمع اسم النطاق الذي استخدمته للوصول إلى الإنترنت، والموقع الإلكتروني الذي جئت منه، والموقع الإلكتروني الذي تزوره بعد ذلك. قد تجمع هذه المعلومات لقياس عدد زيارات الموقع، ومتوسط الوقت المستغرق، ومشاهدات الصفحة، وإحصاءات أخرى حول زوار هذا الموقع. كما قد نستخدم هذه البيانات التي يتم تجميعها لمراقبة أداء الموقع ولجعل الموقع أكثر سهولة وملاءمة للاستخدام". (جامعة القدس المفتوحة. سياسة الخصوصية، ٢٠٢٢)

٢/٤/١ سياسات حماية خصوصية بيانات المستخدمين بالمكتبات الأكاديمية عالميًا:

■ **الولايات المتحدة الأمريكية:** على الرغم من عدم سن قانون خاص بحماية خصوصية البيانات في الولايات المتحدة بعد قانون الخصوصية للعام ١٩٧٤ إلا أنها من أكثر الدول اهتمامًا بحماية خصوصية بيانات المستخدمين في المكتبات الأكاديمية، وتُرجع الدراسة أن ذلك بسبب جهود جمعية المكتبات الأمريكية بشأن القضايا المتعلقة بالخصوصية على مدى الفترات السابقة، كذلك الاهتمام بالقضايا الأخلاقية لمسألة الخصوصية وتأثيرها على الأفراد المتعاملين مع المكتبات الأكاديمية بالولايات المتحدة.

● سياسات الخصوصية لمكتبة جامعة بيتسبرج University of Pittsburgh:

توضح السياسة اتفاقها مع سياسات الخصوصية لجمعية المكتبات الأمريكية ALA وجاءت السياسة كالتالي:

- **بيان خصوصية البيانات:** نقوم بجمع واستخدام وتخزين معلومات محددة عن المستخدمين لتقديم أفضل خدمة، وتحمل المكتبة مسؤولية ضمان الإدارة الآمنة والشفافة لهذه البيانات، فالخصوصية هي القيمة الأساسية للمكتبات، ولا نشارك المعلومات الشخصية مع أطراف ثالثة غير تلك التي تعاقدا معها لتقديم خدمات المكتبة، حيث تخضع هذه الأطراف لمراجعة أمنية من الجامعة.

- **حسابات المُستفيدين:** كل فرد في مجتمع الجامعة لديه حساب للمكتبة Library Account يسمح له بالوصول إلى مواد المكتبة، أو القيام بالاستعارة بين المكتبات، أو دفع غرامات المكتبة؛ يتم الحصول على معلومات إنشاء الحساب من الملفات المؤسسية لجامعة بيتسبرج ويتم تخزينها بشكل آمن داخل مراكز البيانات بالجامعة، وبعد إعادة المواد المستعارة من المجموعات المادية للمكتبة، تقوم المكتبة بإزالة جميع الروابط بين حسابك والعناصر التي قمت باستعارتها.

- **الجهات الخارجية:** تسعى المكتبة إلى تغطية احتياجات مستفيديها من قواعد البيانات عن طريق توفير قواعد بيانات للكتب ومنصات إلكترونية عبر مواقع الويب، وتبذل المكتبة قصارى جهدها لحماية خصوصيتك عند التفاوض على التراخيص مع جهات خارجية؛ لذلك يجب ملاحظة أن المكتبة الأكاديمية لجامعة بيتسبرج غير مسؤولة عن ممارسات الخصوصية أو محتوى أدوات الجهات الخارجية (الموردين)، وعليه يجب قراءة السياسات المرتبطة بالخصوصية للجهات الخارجية قبل استخدامها؛ فقد تتطلب بعض مواقع الويب أو قواعد البيانات تسجيلًا إضافيًا لدى المورد الذي قد يطلب معلومات شخصية. (University of Pittsburgh. Data privacy statement, 2022)

• سياسات الخصوصية لمكتبة جامعة هارفارد Harvard University:

تلتزم مكتبة جامعة هارفارد بحماية خصوصية مستخدميها، وتتفق مع سياسات الخصوصية المدونة قواعد الأخلاق لجمعية المكتبات الأمريكية Code of Ethics of the American Library Association، وتوضح سياسات المكتبة أنها تستخدم خدمة تحليل الويب من جوجل Google Analytics؛ يتم استخدام المعلومات التي تم جمعها لتحسين خدمات الويب للمستخدمين من خلال ملفات تعريف الارتباط Cookies والتي يمكن إيقافها في أي وقت من خلال إعدادات التفضيلات في المتصفح.

قد تُخزن المكتبة معلومات التعريف الشخصية مع عمليات الإعارة العادية أو الخدمات الأخرى؛ وقد تكون المكتبة مُلزَمة بالإفصاح عن هذه المعلومات إلى العملاء الفيدراليون ردًا على أمر تفتيش أو أمر استدعاء صادر وفقًا لقانون مراقبة الاستخبارات الأجنبية بصيغته المعدلة بقانون باتريوت الأمريكي؛ والخاص بمكافحة الإرهاب، حيث يحظر هذا القانون على موظفي المكتبة إبلاغك باستلام مثل هذا الطلب، وهو ما يعتبر انتهاكًا لخصوصية بيانات المستخدمين بشكل صريح وواضح ضمن السياسة مما يُعطل عمليات إصدار تشريعات وقوانين تخص حماية خصوصية البيانات بالولايات المتحدة الأمريكية.

لتنطبق السياسة بعد ذلك فيما يخص سياسة خصوصية استخدام المصادر الإلكترونية؛ تتفق أيضًا مع مدونة أخلاقيات جمعية المكتبات الأمريكية من حيث البيانات التي يتم جمعها في كل جلسة وفقًا لطريقة الاتصال بالموارد، وتحتوي الملفات المُجمعة على المعلومات اللازمة لتحليل استخدام الموارد واستكشاف المشكلات وإصلاحها وتحسين الخدمات، ويمتد الالتزام ليشمل موردي الخدمات الإلكترونية وقواعد البيانات من خلال الاطلاع على سياسات الموردين على المواقع الخاص بهم.

وتُشير سياسات المحتوى الرقمي، وقاعدة بيانات الصور والمواد المرئية والخاصة بمكتبات جامعة هارفارد "العارض The viewer" إلى توفير المحتوى للاستخدام الشخصي غير التجاري لأغراض التدريس والبحث، ولا يجوز النسخ أو النشر أو التوزيع أو العرض أو الإتاحة لأي محتوى محمي بموجب حقوق النشر، باستثناء ما قد يُسمح به بموجب الاستخدام العادل أو استثناء آخر لقانون حقوق النشر؛ وفي حالة الرغبة في استخدام أي محتوى من هذا القبيل، فيجب الحصول على إذن من صاحب حقوق النشر، والذي قد يكون هارفارد أو طرف آخر. (HARVARD LIBRARY. PRIVACY STATEMENT, 2022)

• سياسات الخصوصية لمكتبة جامعة بيركلي بكاليفورنيا UC Berkeley Library:

حيث تنص سياسة "مكتبات جامعة كاليفورنيا بيركلي" على احترام خصوصية جميع المستخدمين وفقًا للقوانين الفيدرالية وقوانين الولايات المتحدة الأمريكية، وكذلك المعايير المهنية؛ وجاءت كالتالي:

لن تكشف المكتبة عن معلومات التعريف الشخصية للمستخدمين الفرديين أو تكشف عن مصادر المعلومات أو الكتب التي يقومون باستعارتها، وتشمل أسباب الإفصاح أن يكون المُستفيد مطلوبًا بموجب أمر تفتيش أو أمر استدعاء، أو إذا كان هناك سبب موثق لحدوث انتهاكات للقانون أو سياسات الجامعة أو الحرم الجامعي أو المكتبة؛ أو عندما يؤدي التصرف إلى ضرر جسدي كبير أو خسارة كبيرة في الممتلكات التي تخص المكتبة.

كما تنطبق هذه السياسة على جميع المصادر بغض النظر عن شكلها أو وسيلة إيصالها وكذلك على جميع الخدمات التي تقدمها المكتبة، وتعتبر جميع ملفات المكتبة والمعلومات الأخرى المجمعَة والمتعلقة باستخدام المُستفيد للمكتبة ومصادر سرية؛ تتضمن هذه الملفات ملفات الإعارة بالمكتبة، والعنوان ومعلومات التسجيل الأخرى، والأسئلة المرجعية أو المعلوماتية المطروحة، ومعاملات الإعارة بين

المكتبات، وعمليات البحث في قاعدة بيانات الكمبيوتر، ويمكن الرجوع إليها واستخدامها من قبل موظفي المكتبة في سياق القيام بأعمال المكتبة. (UC Berkeley Library. Privacy Policy, 2022)

كندا :Canada:

سياسات الخصوصية لمكتبة جامعة ماكجيل :McGill University

توضح السياسة ان الدور الرئيسي الذي تقوم به المكتبة هو حماية خصوصية بيانات مُستفيديها، فالمكتبة هي مكان يمكن للأشخاص من خلاله البحث عن المعلومات ومشاركتها بحرية، وفي نفس الوقت فإن معلوماتهم الشخصية محمية وسرية، وأوضحت بأن الغرض من السياسة هو توضيح كيفية عمل هذه الإجراءات على تحقيق هدف حماية الخصوصية لمُستفيديها؛ وقُسمت السياسة إلى:

- **المعلومات الشخصية:** تظل المعلومات الشخصية التي تقدمها عبر استمارات الموقع والبريد الإلكتروني سرية دائماً، ومن الأمثلة على هذه المعاملات التسجيل في ورشة عمل بالمكتبة أو تقديم طلب شراء؛ حيث تُستخدم هذه المعلومات فقط لأغراض تقديم الخدمة المطلوبة، فالمكتبة لا تجمع المعلومات لأغراض التسويق التجاري.

- **الموقع الإلكتروني:** إذا قمت بزيارة الموقع الإلكتروني للمكتبة، بغض النظر عن سبب الزيارة سواء كانت اطلاع أو تنزيل ملفات، فإننا نقوم تلقائياً بجمع وتخزين المعلومات التي يتم تسجيلها بواسطة خوادم الويب، بما في ذلك عنوان IP للمُستفيد وتاريخ ووقت الطلب والصفحة المطلوبة والصفحات التي قُمت بزيارتها، حيث يتم جمع هذه المعلومات دائماً بشكل إجمالي ولا تحدد هويتك شخصياً.

- **البحث في فهرس المكتبة الإلكترونية:** عند إجراء البحث في فهرس المكتبة الإلكتروني فإن جمع عمليات البحث يتم بشكل إجمالي بواسطة مورد الخدمة (الطرف الثالث)، مما يعني أن عمليات البحث الفردية لا تُظهر بيانات من قام بالبحث شخصياً. كما تُوضح السياسة أن المكتبة تستخدم خدمة تحليل الويب من جوجل Google Analytics للمساعدة في تحليل كيفية استخدام الزوار لموقع المكتبة والفهرس الإلكتروني. حيث تجمع خدمة جوجل وتوفر رؤية أوضح للبيانات مجهولة المصدر التي تم جمعها أثناء جلسة تصفح المستخدم، كما قد تتضمن البيانات أنماط التنقل (بما في ذلك الروابط التي تم النقر عليها والصفحات التي تمت زيارتها)، ومنطقة المنشأ (بناءً على IP)، ومصدر الزيارات (مثل الإحالات)، وتفضيل اللغة، ونوع المتصفح، وحجم الشاشة، من خلال استخدام ملفات تعريف الارتباط Cookies، وهي ملفات نصية موضوعة على جهاز الكمبيوتر الخاص بالمُستفيد، لجمع معلومات سجل الإنترنت القياسية ومعلومات سلوك الزائر في شكل مجهول، وتستخدم المكتبة هذه المعلومات لفهم أفضل لكيفية استخدام الزوار لموقع المكتبة ولتحسين الخدمات.

- **ملفات المكتبة:** تعتبر بيانات الإعارة حول استعارة أو استخدام المواد من مجموعة المكتبة سرية تماماً، ويتم الاحتفاظ بها لمدة أقصاها خمسة أشهر، كما يمكن طلب معلومات حول تاريخ الاستعارة الأخير الخاص بك من الموظفين في مكتب خدمات المكتبة، وتُعامل الملفات الأخرى الخاصة بتفاعلات المستخدمين داخل المكتبة سرية أيضاً، والتي تشمل: معاملات الغرامات والرسوم، والمعاملات المرجعية سواء كانت مكتوبة، أو هاتفية، أو من خلال البريد الإلكتروني.

- **مُوردي المكتبة أو الطرف الثالث:** حيث توضح المكتبة أنها تتعامل مع موردين خارجيين لتقديم خدمات قواعد البيانات ومنصات الكتب الإلكترونية، وتوجه عناية المُستفيدين بضرورة ملاحظة أن هؤلاء المُوردين قد يكون لها سياسات مختلفة فيما يتعلق بجمع البيانات والمشاركة، لذا يُرجى

التأكد من قراءة سياسة الخصوصية المرتبطة بهم. (McGill Library. Privacy Statement, 2022)

استراليا:

• **سياسة الخصوصية لمكتبة جامعة نيو ساوث ويلز سيدني UNSW SYDNEY:**

أوضحت السياسة أن التعامل مع المعلومات التي يتم تجميعها من خلال موقع الجامعة يتم وفقاً لقانون الخصوصية وحماية المعلومات الشخصية لعام ١٩٩٨ وبدأت السياسة بتعريف للبيانات الشخصية كالتالي:

- **المعلومات الشخصية:** يتم تعريف المعلومات الشخصية في القانون على أنها معلومات أو رأي حول فرد تكون هويته واضحة أو يمكن التحقق منها بشكل معقول؛ ومن تلك المعلومات: المعلومات الشخصية كالأسماء والعناوين وأرقام الهواتف وعناوين البريد الإلكتروني وتواريخ الميلاد وأرقام جوازات السفر، وبموجب القانون، لا تعتبر المعلومات المتعلقة بالفرد معلومات شخصية، عندما يتعلق الأمر بشخص مات منذ أكثر من ٣٠ عاماً؛ حيث يمكن ضم معلومات عنه في شكل مطبوعات متاحة للجمهور.

- **جمع المعلومات الشخصية التي تُقدم عن طريق المُستفيد:** توفر جامعة نيو ساوث ويلز تسهيلات التغذية الراجعة على مواقعها الإلكترونية للسماح للمستخدمين بتقديم المُدخلات التي تساهم في تحسين الخدمات مستقبلاً، وعليه يجب على المستخدمين تزويد جامعة نيو ساوث ويلز بالاسم، وعنوان البريد الإلكتروني بغرض تلقي ردًا على ملاحظاتهم، ويتم استخدام هذه المعلومات فقط للغرض الذي تم توفيرها من أجله ولن تتم إضافة اسمك وعنوان بريدك الإلكتروني إلى أي قائمة بريدية من قبل UNSW.

- **الجمع التلقائي للمعلومات الشخصية:** يحق لجامعة نيو ساوث ويلز جمع معلومات شخصية وبيانات أخرى منك من خلال استخدام ملفات تعريف الارتباط Cookies أو غيرها من الوسائل الآلية بما في ذلك ملفات الخادم؛ قد تتضمن المعلومات التي تم جمعها بواسطة UNSW من خلال ملفات تعريف الارتباط والوسائل الأخرى: عنوان الخادم الخاص بك؛ اسم المجال الخاص بك؛ عنوان IP الخاص بك؛ تاريخ ووقت زيارتك؛ الصفحات التي تم الوصول إليها والملفات التي تم تنزيلها؛ الموقع السابق الذي تمت زيارته؛ نوع المتصفح الذي استخدمته، ويمكنك اختيار عدم السماح بملفات تعريف الارتباط من خلال إعدادات متصفح الويب الخاص بك.

- **استخدام والكشف عن المعلومات الشخصية:** تستخدم جامعة نيو ساوث ويلز المعلومات الشخصية التي قدمتها إلى جامعة نيو ساوث ويلز للغرض الأساسي الذي قدمته من أجله ولأغراض ثانوية أخرى مرتبطة مباشرة بهذا الغرض الأساسي. الجامعة ليست مسؤولة عن ممارسات الخصوصية لمواقع الويب الخارجية لجامعة نيو ساوث ويلز، ولن تكشف جامعة نيو ساوث ويلز عن معلوماتك الشخصية دون موافقتك ما لم يأذن القانون بخلاف ذلك، ويجوز لجامعة نيو ساوث ويلز الكشف عن المعلومات الشخصية لطرف ثالث إذا كان الكشف ضرورياً لمنع أو تقليل تهديد خطير ووشيك لحياتك أو صحة شخص آخر.

- **الوصول إلى المعلومات الشخصية الخاصة بك:** لديك الحق في الوصول إلى معلوماتك الشخصية التي تحتفظ بها جامعة نيو ساوث ويلز، ويمكنك طلب تعديل هذه المعلومات إذا كنت تعتقد أنها غير صحيحة، أو لديك سبب للتعديل؛ كما يمكنك تقديم شكاوى حول ممارسات معالجة المعلومات الخاصة بجامعة نيو ساوث ويلز أو انتهاكات خصوصيتك من قبل جامعة نيو ساوث ويلز.

(UNSW SYDNEY. Privacy Policy, 2014)

خاتمة:

توضح الدراسة أن آلية تقديم خدمات المعلومات وقواعد البيانات بالمكتبات يجب أن تُطبق من خلال معايير واضحة تتعامل مع بيانات المُستفيدين بحرص ودقة، لأن المكتبة ستظل المساحة الآمنة والموثوقة لخدمة المُستفيدين وعليه يجب الاهتمام بضبط إجراءات خصوصية بيانات المُستفيدين عند تقديم الخدمات مع الأخذ في الاعتبار القوانين والتشريعات المحلية للدولة ؛ كذلك توافق تلك القوانين والتشريعات مع القوانين الدولية لخصوصية البيانات خاصة في حالة التعامل مع أطراف أخرى من خارج الدولة في تقديم خدمات المعلومات، وأن التعديل على البيانات سواء بالحذف أو الإضافة حق لكل شخص بموجب قوانين حماية خصوصية الأفراد وهو ما توافقت عليه قوانين حماية البيانات بالدول المذكورة في الدراسة، وتبعتها سياسات المكتبات الأكاديمية في هذه الدول.

قائمة المصادر والمراجع العربية

- ١- أبو غزالة، حسام. (٢٠١٩). تعرف على أبرز أهداف قانون حماية البيانات الشخصية. بوابة الوطن. ٢٠١٩/٠٢/١٩. متاح على: <https://bit.ly/39R0Ihd>. تم الاسترداد: ٢٠٢٠/٠٧/١٢.
- ٢- الإمارات العربية المتحدة. البوابة الرسمية لحكومة الإمارات العربية المتحدة. حكومة دبي. مبادرة بيانات دبي (٢٠١٩). متاح على: <https://www.digitaldubai.ae/ar/data>. تم الاسترداد: ٢٠٢٠/٢/١٩.
- ٣- الإمارات العربية المتحدة. وزارة العدل. القانون الاتحادي رقم ١٢ لعام ٢٠١٦ لحماية البيانات والخصوصية. (٢٠١٦). متاح على: <https://bit.ly/3ER9OpI>. تم الاسترداد: ٢٠٢١/١١/١٧.
- ٤- تونس. وزارة العدل. الهيئة العامة لحماية المعطيات الشخصية. قانون رقم ٦٣ لسنة ٢٠٠٤ والمتعلق بحماية المعطيات الشخصية. (٢٠٠٤). القانون الأساسي عدد ٦٣ لسنة ٢٠٠٤ المؤرخ في ٢٧ جويلية ٢٠٠٤ والمتعلق بحماية المعطيات الشخصية. متاح على: <https://bit.ly/3Ofcvo2>. تم الاسترداد: ٢٠٢٠/٧/١٤.
- ٥- جامعة الجوف. السياسة العامة للمكتبات. (٢٠٢١). جامعة الجوف. عمادة شؤون المكتبات الجامعية. سياسات المكتبة. متاح على: <https://bit.ly/3sjeS0q>. تم الاسترداد: ٢٠٢١/١١/١١.
- ٦- جامعة السلطان قابوس. ضوابط السلوك. (٢٠٢٢). ضوابط سلوك مكتبات جامعة السلطان قابوس. متاح على: <https://bit.ly/3KTakjc>. تم الاسترداد: ٢٠٢٢/٤/١٢.
- ٧- جامعة القدس المفتوحة. سياسة الخصوصية. (٢٠٢٢). متاح على: <https://bit.ly/3FwyTWE>. تم الاسترداد: ٢٠٢٢/١٠/٥.
- ٨- جامعة الملك فيصل. سياسة الأمن السيبراني. (٢٠٢١). عمادة تقنية المعلومات. قسم التطوير والجودة. الإصدار الثاني: ٢٠٢١/٧/١٢. متاح على: <https://bit.ly/3krZCU1>. تم الاسترداد: ٢٠٢٢/٥/٨.
- ٩- جامعة الملك فيصل. سياسة الخصوصية. (٢٠٢٠). جامعة الملك فيصل. عمادة تقنية المعلومات. متاح على: <https://bit.ly/394tnyw>. تم الاسترداد: ٢٠٢٢/٤/١٠.
- ١٠- جمهورية مصر العربية. قانون حماية خصوصية البيانات المصري رقم ١٥١ لسنة ٢٠٢٠. (٢٠٢٠). قانون رقم ١٥١ لسنة ٢٠٢٠ بإصدار قانون حماية البيانات الشخصية. الجريدة الرسمية. العدد ٢٨ مكرر (هـ). السنة ٦٣. ١٥ يوليو ٢٠٢٠. متاح على: <https://bit.ly/3ke0UZu>. تم الاسترداد: ٢٠٢٠/٧/١٢.

- ١١- حموري، شهد؛ المصري، ريم. (٢٠١٤). قانون حماية البيانات الشخصية. ما يمكن تعلمه من تجارب الدول الأخرى. متاح على: <https://bit.ly/3Lh1C3O>. تم الاسترداد: ٢٠٢٠/٧/١٢.
- ١٢- خميس، أحمد؛ الطيار، محمد. (٢٠٢١). بريطانيا والبريكست الخشن (التداعيات المستقبلية). الموسوعة الجزائرية للدراسات السياسية والاستراتيجية. متاح على: <https://bit.ly/3Ki1sln>. تم الاسترداد: ٢٠٢١/٨/٢٠.
- ١٣- دراسة نقدية حول قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠. مركز بحوث القانون والتكنولوجيا. كلية القانون. الجامعة البريطانية. الإثنين. ١٢ أكتوبر ٢٠٢٠.
- ١٤- زكي، مصطفى. (٢٠١٨). "حماية البيانات الشخصية". مشروع قانون في صالح المواطن والاستثمار. بوابة الأهرام. ١٠/٠٨/٢٠١٨. متاح على: <https://bit.ly/3njyxu9>. تم الاسترداد: ٢٠٢٠/١١/١٠.
- ١٥- الشامي، خالد. (٢٠١٧). نص مشروع قانون حماية البيانات الشخصية. المصري اليوم. ٢٠١٧/١١/٢٠. متاح على: <https://bit.ly/2H2GCz1>. تم الاسترداد: ٢٠٢٠/٠٧/١٢.
- ١٦- عيد، نيرة. (٢٠١٨). رئيس لجنة التشريعات بوزارة الاتصالات: قانون حماية البيانات الشخصية عنصر جذب للاستثمار في التعهيد. أموال الغد. متاح على: <https://bit.ly/3AdEuQW>. تم الاسترداد: ٢٠٢٠/١٢/٠٧.
- ١٧- فخري، نورا. (٢٠٢٠). مجلس النواب يوافق نهائياً على قانون حماية البيانات الشخصية. اليوم السابع. ٢٠٢٠/٠٢/٢٤. متاح على: <https://bit.ly/39Sd2h9>. تم الاسترداد: ٢٠٢٠/١٢/٠٧.
- ١٨- فضيحة كامبريدج أناليتكا. (٢٠١٨). الادعاء العام في واشنطن يقاضي فيسبوك. BBC NEWS. متاح على: <https://bbc.in/3MXV22B>. تم الاسترداد: ٢٠٢١/٧/٢٧.
- ١٩- قطر. وزارة العدل. قانون رقم (١٣) لسنة ٢٠١٦ بشأن حماية خصوصية البيانات الشخصية. (٢٠١٦). الميزان. البوابة القانونية القطرية. متاح على: <https://bit.ly/3vqhuf7>. تم الاسترداد: ٢٠٢٠/٧/١٤.
- ٢٠- مكتبة قطر الرقمية. سياسة الخصوصية. (٢٠٢١). متاح على: <https://bit.ly/3kR8Wri>. تم الاسترداد: ٢٠١٧/١١/١١.
- ٢١- المملكة الأردنية الهاشمية. ديوان التشريع والرأي. قانون حماية البيانات الشخصية لسنة ٢٠٢٠. (٢٠٢٠). متاح على: <https://bit.ly/3Hx8oBu>. تم الاسترداد: ٢٠٢٢/٦/١٧.
- ٢٢- المملكة المغربية. وزارة العدل. مديرية التشريع. قانون رقم ٠٩،٠٨ لسنة ٢٠٠٩ والمتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي المملكة المغربية. (٢٠٠٩). الجريدة الرسمية عدد ٨١٠٠ بتاريخ ٢١ صفر ٠٣٤٩ (٢٤ فبراير ٢٠٠٩) ص ٨٨٢. متاح على: <https://bit.ly/3QlqK3d>. تم الاسترداد: ٢٠٢٠/٧/١٤.
- ٢٣- وزارة الاتصالات وتكنولوجيا المعلومات. تقرير اللجنة المشتركة من لجنة الاتصالات وتكنولوجيا المعلومات ومكاتب لجان الشئون الدستورية والتشريعية، الخطة والموازنة والدفاع والأمن القومي. (٢٠١٩). جمهورية مصر العربية. مجلس النواب. الفصل التشريعي الأول. دور الانعقاد العادي الرابع. التقرير الثاني. مشترك. متاح على: <https://bit.ly/3MXOfWH>. تم الاسترداد: ٢٠٢٠/٥/٢٨.

- 1- **ALA Statements and Policies .(2017)**. ALA American library association. Privacy. Retrieved from: <https://bit.ly/3cdD6yw> . Available at: 7/4/2020.
- 2- **American University of Beirut AUB. USERS' PRIVACY AND CONFIDENTIALITY. (2016)**. University Libraries Policies and Procedures.Retrieved from: <https://bit.ly/3Fpqzbf>. Available at: 10/4/2022.
- 3- **General Data Protection Regulation GDPR. (2016)**. The European Union. THE EUROPEAN PARLIAMENT. Retrieved from: <https://bit.ly/3FuM2Qe>. Available at: 20/12/2020.
- 4- **HARVARD LIBRARY. PRIVACY STATEMENT. (2022)**. Harvard Library's privacy policy. Privacy, Terms of Use & Copyright Information. Retrieved from: <https://bit.ly/3Ftmjaw>. Available at: 10/4/2022.
- 5- **McGill Library. Privacy Statement. (2022)**. Retrieved from: <https://bit.ly/38idW5w>. available at: 10/4/2022.
- 6- **The University of New South Wales. Privacy Policy UVSW. (2014)**. Retrieved from: <https://bit.ly/39MzCY7>. Available at: 18/4/2022.
- 7- **University of California. Library Privacy Policy. (2022)**. Berkeley Libraries. Retrieved from: <https://bit.ly/3LXCAC>. Available at: 10/4/2022.
- 8- **University of Pittsburgh. Data Privacy Statement. (2022)**. University of Pittsburgh Library System. Retrieved from: <https://bit.ly/3wd83P5>. Available at: 10/4/2022.
- 9- **USA. PATRIOT Act.(2001)**. Financial Crimes Enforcement Network. Retrieved from: <https://bit.ly/3vT5nHz>. Available at: 8/5/2022.
- 10- **USA. Privacy Act Of 1974. (2008)**. (n.d.) West's Encyclopedia of American Law, edition 2. Retrieved from: <https://bit.ly/2LsO8oo>. Available at: 15/5/2020.
- 11- **USA. The California Consumer Privacy Act CCPA. (2018)**. State of California Department of Justice. ROB BONTA. Attorney General. Retrieved from: <https://bit.ly/3FoEnTe>. Available at: 19/7/2021.