

الإشكالية القانونية حول الخصوصية الرقمية في مواجهة استهداف الإعلانات

دراسة تحليلية مقارنة بين بعض التشريعات العربية والغربية

The legal challenges posed by targeted advertising to digital privacy

A comparative analysis of relevant Arab and Western laws

بن سالم سهام (1) بوداود بومدين (2)

(1) جامعة غرداية (الجزائر)، bensalem.siham@univ-ghardaia.dz

(2) جامعة غرداية (الجزائر) boudaoud.boumediene@univ-ghardaia.dz

تاريخ النشر: 2024/12/31

تاريخ القبول: 2023/12/16

تاريخ الاستلام: 2024/09/28

ملخص:

في ظل تطور المشهد الرقمي وزيادة الاعتماد على الإنترنت في مختلف جوانب الحياة برزت العديد من التحديات القانونية والأخلاقية، أبرزها مسألة حماية الخصوصية الرقمية، ففي ظل تزايد حجم البيانات الشخصية التي يتم جمعها وتحليلها من قبل الشركات والمؤسسات في البيئة الرقمية، أصبح استهداف الإعلانات دقيقاً للغاية، مما يثير مخاوف وتساؤلات حول مدى احترام خصوصية الأفراد وحقوقهم في التحكم في بياناتهم الشخصية، يهدف هذا البحث إلى دراسة الإشكالية القانونية التي تنشأ عن التعارض بين حق الأفراد في الخصوصية الرقمية وحق الشركات والمؤسسات في استهداف الإعلانات، وذلك من خلال إجراء مقارنة تحليلية بين بعض التشريعات العربية والغربية في هذا المجال انطلاقاً من إشكالية رئيسية تتمثل في التحدي القائم حول مدى تحقيق التوازن بين حماية الخصوصية الرقمية للأفراد وحق الشركات في ممارسة أنشطتها التجارية عبر الإنترنت

الكلمات المفتاحية: الخصوصية الرقمية، الإشهار الإلكتروني، المستهلك، الإعلانات، التشريعات والقوانين

Abstract :

As the digital landscape evolves and internet reliance grows across various aspects of life, numerous legal and ethical challenges have emerged, most notably the issue of digital privacy. With the increasing volume of personal data being collected and analyzed by companies and institutions within the digital environment, targeted advertising has become highly precise. This raises concerns and questions about the extent to which individuals' privacy is respected and their right to control their personal data. This research aims to examine the legal dilemma arising from the conflict

between individuals' right to digital privacy and the right of companies and institutions to engage in targeted advertising. It will do so by conducting a comparative analysis of relevant legislation in both Arab and Western countries. The central challenge lies in striking a balance between protecting individuals' digital privacy and enabling companies to conduct their online businesses.

Keywords: digital privacy, online advertising, consumer, advertisements, legislation, laws.

مقدمة

يشهد عالمنا اليوم تحولاً رقمياً متسارعاً، حيث أصبحت التكنولوجيا جزءاً لا يتجزأ من حياتنا اليومية، ومع هذا التطور الهائل، برزت تحديات جديدة تهدد خصوصيتنا، أبرزها الانتشار الواسع لممارسات استهداف الإعلانات. ففي مقابل الفوائد التي تجنيها الشركات من خلال هذه الممارسات، والتي تتمثل في زيادة كفاءة الحملات الإعلانية وتحقيق عائد استثمار أعلى، يواجه الأفراد تهديداً مباشراً لخصوصياتهم، حيث يتم تتبع سلوكهم على الإنترنت وجمع بياناتهم الشخصية لتحليلها واستخدامها في توجيه الإعلانات إليهم بشكل مخصص.

تكمن خطورة هذه الممارسات في أنها تتعدى مجرد عرض إعلانات مزعجة، بل تتغلغل في أعماق حياتنا الرقمية، حيث يتم بناء ملفات تعريف تفصيلية لكل فرد بناءً على بياناته الشخصية وسلوكياته، مما يتيح للشركات استهدافنا بإعلانات مصممة خصيصاً للتأثير على قراراتنا وسلوكياتنا الاستهلاكية، هذا الأمر يثير تساؤلات جدية حول مدى احترام خصوصيتنا في ظل هذا التطور التكنولوجي المتسارع، وحقنا في التحكم في بياناتنا الشخصية ومنع استخدامها دون موافقتنا.

في ظل هذا المشهد المعقد، يبرز التناقض بين الحاجة الملحة لحماية الخصوصية من جهة، والمصالح الاقتصادية الكبيرة التي تدفع الشركات إلى استغلال البيانات الشخصية من جهة أخرى، هذا التناقض يطرح إشكالية قانونية معقدة تتطلب دراسة متأنية للقوانين والتشريعات التي تحكم هذا المجال في مختلف البلدان، لا سيما في ظل التباين الكبير بين التشريعات العربية والغربية في هذا الصدد، ففي حين تسعى بعض الدول إلى وضع قوانين

الإشكالية القانونية حول الخصوصية الرقمية في مواجهة استهداف الإعلانات

صارمة لحماية الخصوصية، تبقى دول أخرى مترددة في فرض قيود على ممارسات الشركات، مما يخلق بيئة غير متجانسة وتزيد من صعوبة حماية الخصوصية على المستوى العالمي.

إشكالية الدراسة:

تطرح الدراسة إشكالية توازن دقيق بين الحق الفردي في الخصوصية الرقمية وبين المصالح الاقتصادية للشركات التي تعتمد على جمع وتحليل البيانات الشخصية لتوجيه الإعلانات، ففي ظل التطور التكنولوجي المتسارع وانتشار ممارسات استهداف الإعلانات، يتعرض الأفراد لانتهاكات متزايدة لخصوصياتهم، هذا التناقض يفرض تحديات قانونية كبيرة، خاصة مع تباين التشريعات بين الدول العربية والغربية في التعامل مع هذه القضية، مما يثير تساؤلات حول الكيفية التي يمكن من خلالها حماية الخصوصية الرقمية وضمان حقوق الأفراد دون الإضرار بالابتكار الاقتصادي، وبالتالي الدراسة تطرح سؤالاً جوهرياً: كيف يمكن تحقيق التوازن بين حماية الخصوصية الرقمية وضمان بيئة رقمية مبتكرة تدعم النمو الاقتصادي، خاصة في ظل التباين الكبير في التشريعات بين الدول العربية والغربية؟

تساؤلات الدراسة:

- ما هي أبرز التحديات التي تواجه حماية الخصوصية الرقمية في ظل انتشار استهداف الإعلانات؟

- كيف تتعامل التشريعات العربية والغربية مع هذه التحديات؟

- ما هي نقاط القوة والضعف في هذه التشريعات؟

- ما هي التوصيات التي يمكن تقديمها لتعزيز حماية الخصوصية الرقمية في العالم العربي؟

أهداف الدراسة:

- مقارنة بين هذه التشريعات لتحديد نقاط التشابه والاختلاف، وتقييم مدى كفاءتها في

حماية الخصوصية في ظل التطور التكنولوجي المتسارع.

- تحديد الثغرات والقصور في هذه التشريعات، واقتراح التعديلات اللازمة لسد هذه الثغرات.

- تحديد أبرز التحديات القانونية والتقنية التي تواجه حماية الخصوصية الرقمية في ظل انتشار ممارسات استهداف الإعلانات.

- دراسة دور التكنولوجيا الحديثة، مثل الذكاء الاصطناعي، في تعقيد هذه التحديات.

منهج الدراسة وأدواتها وعينتها:

تستخدم الدراسة المنهج التحليلي المقارن لتحديد تباين التشريعات العربية والغربية المتعلقة بحماية الخصوصية الرقمية واستهداف الإعلانات، حيث سيتم جمع البيانات من مصادر مختلفة مثل القوانين واللوائح، والأبحاث السابقة، والمقالات العلمية، وتقارير المنظمات الدولية، إلى جانب تحليل البيانات بشكل مقارن لتحديد أوجه التشابه والاختلاف بين التشريعات، وتقييم مدى تطابقها مع المعايير الدولية لحماية البيانات.

كما تستخدم الدراسة المنهج الوصفي فيما يتعلق بالوضع الراهن لحماية الخصوصية الرقمية في الدول العربية والغربية، وذلك من خلال تحليل النصوص القانونية والقوانين واللوائح ثم مقارنة التشريعات المختلفة وتحديد أوجه التشابه والاختلاف.

أما عينة الدراسة فتشمل التشريعات والقوانين المتعلقة بحماية البيانات الشخصية والخصوصية الرقمية في مجموعة من الدول العربية والغربية، ويتم اختيارها وفق معايير محددة حسب مستوى التطور التكنولوجي والاقتصادي، وحسب أنظمة قانونية مختلفة، وحسب تجربة كل بلد في مجال حماية البيانات.

المفاهيم الإجرائية للدراسة:

أ- الخصوصية الرقمية:

تعد الخصوصية الرقمية حقًا أساسيًا من حقوق الإنسان، وهي تتعدى مفهومها التقليدي لتشمل الحق في التحكم في المعلومات الرقمية التي تتعلق بالفرد¹، بدءًا من البيانات

الإشكالية القانونية حول الخصوصية الرقمية في مواجهة استهداف الإعلانات

الشخصية الأساسية كاسم وعنوان وصولاً إلى بيانات أكثر تفصيلاً عن سلوكياتنا وتفضيلاتنا عبر الإنترنت²، هذا الحق يشمل:

- الحق في الوصول إلى البيانات: أي حق الفرد في الاطلاع على البيانات التي تجمع عنه، ومعرفة كيفية استخدامها.

- الحق في تصحيح البيانات: أي حق الفرد في تصحيح أي معلومات خاطئة أو غير كاملة عنه³.

- الحق في حذف البيانات: أي حق الفرد في طلب حذف بياناته الشخصية من قواعد البيانات المختلفة.

- الحق في الاعتراض على معالجة البيانات: أي حق الفرد في الاعتراض على استخدام بياناته لأغراض معينة، مثل التسويق المباشر⁴.

ب- أهمية الخصوصية الرقمية:

- تساعد الخصوصية الرقمية على حماية الهوية الشخصية للأفراد من الانتحال والاحتيال⁵.

- تساعد الخصوصية الرقمية على حماية العلاقات الاجتماعية من التدخل الخارجي.

- تساعد الخصوصية الرقمية على حماية الأمن القومي من خلال منع تسريب المعلومات الحساسة.

ج- استهداف الإعلانات

استهداف الإعلانات هو عملية معقدة تتضمن جمع وتحليل كميات هائلة من البيانات الشخصية للمستخدمين، ثم استخدام هذه البيانات لتحديد الإعلانات الأكثر ملاءمة لعرضها على كل مستخدم على حدة. هذه العملية تتم من خلال:

- جمع البيانات: يتم جمع البيانات من مصادر متعددة مثل مواقع الويب، تطبيقات الهاتف المحمول، وشبكات التواصل الاجتماعي.

- تحليل البيانات: يتم تحليل البيانات باستخدام خوارزميات معقدة لتحديد اهتمامات المستخدمين وسلوكياتهم⁶.

- تخصيص الإعلانات: يتم عرض الإعلانات التي تتناسب مع اهتمامات وسلوكيات المستخدم، مما يزيد من فرص تحويل المتصفحين إلى عملاء.

د- أنواع استهداف الإعلانات:

- استهداف ديموغرافي: يستند إلى معلومات ديموغرافية مثل العمر والجنس والتعليم والدخل.

- استهداف سلوكي: يستند إلى سلوك المستخدم على الإنترنت، مثل المواقع التي يزورها والمنتجات التي يبحث عنها.

- استهداف سياقي: يستند إلى محتوى الصفحة التي يعرض عليها الإعلان.

ه- أثر استهداف الإعلانات على الخصوصية: يؤثر استهداف الإعلانات بشكل كبير على الخصوصية الرقمية، حيث يتيح للشركات تتبع الأفراد عبر الإنترنت وجمع معلومات دقيقة عنهم، مما يهدد حريتهم في اتخاذ القرارات ويزيد من فرص تعرضهم للاستغلال.

و- التشريعات ذات الصلة: تشمل التشريعات ذات الصلة بالخصوصية الرقمية واستهداف الإعلانات مجموعة واسعة من القوانين واللوائح التي تغطي جوانب مختلفة من هذه القضية⁷، مثل: قوانين حماية البيانات الشخصية: تهدف هذه القوانين إلى حماية البيانات الشخصية للأفراد من جمعها واستخدامها وإفشاءها دون موافقتهم، وقوانين حقوق المؤلف: تحمي حقوق الملكية الفكرية للمبدعين، وتحد من استخدام المحتوى الرقمي دون إذن، وقوانين التجارة الإلكترونية: تنظم المعاملات التجارية التي تتم عبر الإنترنت، وتضمن حقوق المستهلكين، إلى قوانين حماية المستهلك التي تهدف إلى حماية المستهلكين من الممارسات التجارية غير العادلة، مثل الإعلانات المضللة⁸.

ز- أهمية التشريعات ذات الصلة:

تلعب التشريعات دورًا حاسمًا في تحقيق التوازن بين حماية الخصوصية الرقمية وتعزيز النمو الاقتصادي، فهي توفر الإطار القانوني اللازم لحماية حقوق الأفراد، وتحدد من ممارسات الشركات التي تنتهك الخصوصية، وتشجع على المنافسة العادلة في السوق الرقمية.

الدراسة التحليلية المقارنة:

أولاً: التشريعات العربية المتعلقة بالخصوصية الرقمية في مواجهة استهداف

الإعلانات:

1. التشريعات المصرية:

وهنا ستمم الإشارة إلى نصين قانونين وهما:

قانون حماية البيانات الشخصية:

تاريخ الإصدار: صدر القانون رقم 152 لسنة 2020⁹ بشأن حماية البيانات الشخصية،

وهو يعد خطوة مهمة في مجال حماية البيانات الشخصية في مصر.

الأحكام الرئيسية:

- تعريف البيانات الشخصية: حدد القانون البيانات الشخصية بشكل واسع لتشمل أي معلومات يمكن استخدامها لتحديد هوية شخص طبيعي بشكل مباشر أو غير مباشر.
- مبادئ حماية البيانات: نص القانون على مبادئ أساسية لحماية البيانات مثل المشروعية، والنزاهة، والشفافية، والحد من الغرض، وتخزين البيانات لفترة محددة، والدقة، والسلامة، والسرية.

- حقوق الأفراد: منح القانون للأفراد مجموعة من الحقوق الأساسية، بما في ذلك:

- الحق في الوصول إلى البيانات الشخصية الخاصة بهم، الحق في تصحيح البيانات غير الدقيقة، الحق في حذف البيانات، الحق في الاعتراض على معالجة البيانات، الحق في نقل البيانات، وقد فرض القانون على المشغلين (أي الجهات التي تقوم بجمع ومعالجة البيانات

الشخصية) مجموعة من الواجبات، مثل إجراء تقييم الأثر على الخصوصية، وتعيين مسؤول حماية البيانات، والإبلاغ عن أي خروقات للبيانات.

النقد والتقييم:

يعتبر القانون خطوة إيجابية في مجال حماية البيانات الشخصية في مصر، حيث يوفر إطارًا قانونيًا واضحًا لحماية حقوق الأفراد، ولا يزال هناك بعض النقاط التي تحتاج إلى مزيد من التوضيح والتطوير، مثل بعض المصطلحات المستخدمة في القانون تحتاج إلى تعريف أكثر دقة ووضوحًا، وأيضًا تحتاج آليات تنفيذ القانون إلى مزيد من التفعيل، بما في ذلك إنشاء هيئة مستقلة للرقابة على تطبيق القانون، ويجب تحقيق توازن بين حماية الخصوصية وتشجيع الابتكار في مجال التكنولوجيا.

القانون المصري لمكافحة جرائم تقنية المعلومات:

- تاريخ الإصدار: صدر القانون¹⁰ رقم 175 لسنة 2018 بشأن تنظيم استخدام المعلومات.

- الأحكام الرئيسية: يهدف القانون إلى تنظيم استخدام المعلومات وتداولها، وحماية الحقوق المتعلقة بالمعلومات، وتنمية صناعة المعلومات، وتعزيز الشفافية والمساءلة في التعامل مع المعلومات،

- أما العلاقة بالخصوصية الرقمية، فهو يتداخل القانون مع قانون حماية البيانات الشخصية في بعض النقاط، خاصة فيما يتعلق بحماية البيانات الشخصية، ولم يتطرق القانون بشكل مفصل إلى قضية الخصوصية الرقمية والإعلانات المستهدفة، مما يترك ثغرات قانونية في هذا المجال.

الجدول رقم 01: مقارنة بين القانونين (النموذج المصري)

الميزة	قانون حماية البيانات الشخصية	قانون تنظيم استخدام المعلومات

الإشكالية القانونية حول الخصوصية الرقمية في مواجهة استهداف الإعلانات

الهدف الرئيسي	حماية البيانات الشخصية للأفراد	تنظيم استخدام المعلومات وتداولها
النطاق	يركز على البيانات الشخصية	يشمل نطاقاً أوسع من المعلومات
الأحكام التفصيلية	يحتوي على أحكام تفصيلية بشأن حقوق الأفراد وواجبات المشغلين	يحتوي على أحكام أكثر عمومية
الخصوصية الرقمية	يتناول الخصوصية الرقمية بشكل مباشر	لا يتناول الخصوصية الرقمية بشكل تفصيلي

المصدر: الباحثان

تهدف التشريعات المصرية الجديدة، ولا سيما قانون حماية البيانات الشخصية وقانون تنظيم استخدام المعلومات، إلى مواكبة التطورات التكنولوجية المتسارعة وحماية الحق في الخصوصية الرقمية، ومع ذلك، تظهر بعض الفجوات والتحديات التي تتطلب مزيداً من التطوير، ما يمكن استخلاصه من النموذج المصري:

يُمثل قانون حماية البيانات الشخصية خطوة جوهرية في حماية حقوق الأفراد في مصر، حيث يوفر إطاراً قانونياً واضحاً لمعالجة البيانات الشخصية، كما يغطي القانون نطاقاً واسعاً من القضايا المتعلقة بحماية البيانات، ولكنه لا يزال بحاجة إلى مزيد من التوضيح والتطوير في بعض الجوانب، مثل تعريفات بعض المصطلحات وآليات التنفيذ، وأيضاً يسعى القانون إلى تحقيق توازن دقيق بين حماية الخصوصية وتشجيع الابتكار في مجال التكنولوجيا، ولا يعالج قانون تنظيم استخدام المعلومات قضية الإعلانات المستهدفة بشكل كافٍ، مما يترك ثغرات قانونية في هذا المجال الحيوي، كما يتداخل قانون حماية البيانات الشخصية مع قانون تنظيم استخدام المعلومات في بعض النقاط، مما يدل على الحاجة إلى مزيد من التنسيق والتكامل بين التشريعات المختلفة.

التحديات المستقبلية:

يتطلب تطبيق القانون آليات تنفيذ فعالة، بما في ذلك إنشاء هيئة مستقلة للرقابة على تطبيق القانون وتوعية الأفراد والشركات بحقوقهم وواجباتهم كما يجب تحديث التشريعات بشكل مستمر لمواكبة التطورات السريعة في مجال التكنولوجيا، مثل الذكاء الاصطناعي وإنترنت الأشياء.

✓ حماية البيانات في سياق الإعلانات المستهدفة: يتطلب تطوير آليات واضحة لتنظيم جمع واستخدام البيانات الشخصية في سياق الإعلانات المستهدفة، مع ضمان حقوق الأفراد في الخصوصية.

✓ التعاون الدولي: يتطلب حماية البيانات في العصر الرقمي التعاون الدولي بين الدول لتطوير معايير مشتركة وحماية البيانات عبر الحدود.

2. التشريعات السعودية:

يشكل نظام حماية البيانات الشخصية في المملكة العربية السعودية خطوة مهمة نحو حماية خصوصية الأفراد في ظل التطور الرقمي المتسارع. يهدف هذا النظام إلى تنظيم جمع ومعالجة البيانات الشخصية، وتاريخ البدء: بدأ العمل بنظام حماية البيانات الشخصية في المملكة العربية السعودية بشكل كامل في 14 سبتمبر 2021.

✓ النطاق: يشمل النظام جميع الكيانات العاملة في المملكة، وكذلك الكيانات الأجنبية التي تعالج بيانات شخصية للأفراد المتواجدين في المملكة.

✓ تعريف البيانات الشخصية من خلال هذا النظام: تشمل البيانات الشخصية أي معلومات يمكن استخدامها لتحديد هوية شخص بشكل مباشر أو غير مباشر، مثل الاسم، ورقم الهوية، والعنوان، والبيانات الصحية، والبيانات الوراثية.

✓ الحقوق التي يمنحها النظام للأفراد:

- الحق في معرفة البيانات الخاصة بهم.

الإشكالية القانونية حول الخصوصية الرقمية في مواجهة استهداف الإعلانات

- الحق في تصحيح البيانات غير الدقيقة.
 - الحق في حذف البيانات.
 - الحق في الاعتراض على معالجة البيانات.
 - الحق في نقل البيانات.
 - ✓ عواقب المخالفة: تصل العقوبات على انتهاك النظام إلى غرامات مالية كبيرة، والحبس في بعض الحالات.
 - ✓ التوافق مع التشريعات الدولية: يتماشى النظام مع التشريعات الدولية المماثلة، مثل اللائحة العامة لحماية البيانات في الاتحاد الأوروبي.
 - ✓ أهمية الامتثال: يعتبر الامتثال للنظام ضروريًا لحماية الأفراد ودعم الاقتصاد الرقمي في المملكة.
- الإجراءات اللازمة للالتزام بالنظام:**
- تحديد وحصر البيانات: يجب على المؤسسات تحديد جميع البيانات الشخصية التي تجمعها وتخزنها.
 - تقييم المخاطر: يجب إجراء تقييم شامل للمخاطر التي قد تهدد أمن البيانات الشخصية.
 - تطوير سياسات وإجراءات: يجب وضع سياسات وإجراءات واضحة لحماية البيانات الشخصية.
 - التدريب: يجب تدريب الموظفين على أهمية حماية البيانات وكيفية التعامل معها بشكل آمن.
 - التقنيات الأمنية: يجب تطبيق أحدث التقنيات الأمنية لحماية البيانات.
- فوائد النظام**
- حماية الخصوصية: يوفر النظام حماية قوية لخصوصية الأفراد.

- الثقة: يعزز النظام ثقة الأفراد والمؤسسات في التعاملات الرقمية.
- الاستثمار: يجذب النظام الاستثمارات الأجنبية ويدعم التحول الرقمي في المملكة.
- التوافق الدولي: يجعل السعودية أكثر تنافسية على الصعيد الدولي.

يمثل نظام حماية البيانات الشخصية في المملكة العربية السعودية خطوة بالغة الأهمية نحو حماية خصوصية الأفراد في ظل التطور المتسارع للتكنولوجيا الرقمية: يهدف هذا النظام الشامل، الذي بدأ تطبيقه في سبتمبر 2023، إلى تنظيم جمع ومعالجة البيانات الشخصية، وتوفير ضمانات قوية لحقوق الأفراد في التحكم ببياناتهم الشخصية: من خلال منحه للأفراد حقوقاً واضحة مثل الحق في الوصول إلى بياناتهم وتصحيحها وحذفها، يساهم النظام في تعزيز الثقة في التعاملات الرقمية ويحمي الأفراد من الاستخدام غير المشروع لبياناتهم: بالإضافة إلى ذلك، فإن التوافق مع المعايير الدولية لحماية البيانات يعزز مكانة المملكة كوجهة جاذبة للاستثمارات ويحفز التحول الرقمي: ومع ذلك، يتطلب نجاح هذا النظام تضافر جهود جميع الأطراف المعنية، من الحكومة إلى المؤسسات والشركات والأفراد، لضمان تطبيقه الفعال وتوعية المجتمع بأهميته.

ثانياً: التشريعات الغربية المتعلقة بالخصوصية الرقمية في مواجهة استهداف

الإعلانات

ونستعرض هنا ثلاث نماذج:

1. اللوائح الأوروبية لحماية البيانات¹² (GDPR):

تعتبر اللائحة العامة لحماية البيانات (GDPR) التي تم اعتمادها في الاتحاد الأوروبي عام 2016 من أهم التشريعات التي شكلت معالم حماية البيانات الشخصية في العالم الرقمي، وقد أحدثت هذه اللائحة تغييرات جذرية في الطريقة التي تجمع بها الشركات البيانات وتستخدمها، خاصة في مجال الإعلانات الرقمية.

أهم مبادئ GDPR

الإشكالية القانونية حول الخصوصية الرقمية في مواجهة استهداف الإعلانات

- يجب الحصول على موافقة صريحة وواضحة من الأفراد قبل جمع ومعالجة بياناتهم الشخصية.
 - يجب أن تكون الشركات شفافة بشأن كيفية جمع البيانات واستخدامها¹³، وأن توفر معلومات واضحة وموجزة للفرد.
 - يجب أن يكون جمع البيانات واستخدامها مقصوداً على أغراض محددة وواضحة.
 - يجب على الشركات اتخاذ جميع التدابير التقنية والتنظيمية اللازمة لحماية البيانات الشخصية¹⁴ من أي انتهاكات.
 - تمنح اللائحة للأفراد مجموعة من الحقوق الأساسية، بما في ذلك الحق في الوصول إلى البيانات، وتصحيحها، وحذفها، والاعتراض على معالجتها.
- تأثير الـ GDPR على صناعة الإعلانات الرقمية:**
- أدت الـ GDPR إلى تغيير جذري في نموذج الأعمال المعتمد على جمع البيانات واستهداف الإعلانات بشكل واسع.
 - فرضت الـ GDPR تكاليف كبيرة على الشركات، خاصة الشركات الكبرى، لتطوير أنظمة وتقنيات جديدة لضمان الامتثال.
 - أصبح جمع البيانات واستخدامها لأغراض التسويق أكثر صعوبة، حيث يتعين على الشركات الحصول على موافقة صريحة من الأفراد.
 - تحولت العديد من الشركات إلى الاعتماد على الإعلانات السياقية التي تعتمد على سياق البحث بدلاً من استهداف المستخدمين بناءً على بياناتهم الشخصية.
 - أدت الـ GDPR إلى تطوير تقنيات جديدة لحماية الخصوصية، مثل التشفير المتقدم والتعلم الآلي.

الجدول رقم 02: التسلسل الزمني لأهم التطورات التشريعية في مجال حماية البيانات

التاريخ	الحدث
---------	-------

1981	صدور الاتفاقية 108 لمجلس أوروبا بشأن حماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية.
1995	صدور التوجيه الأوروبي EC 46/95 بشأن حماية الأفراد الطبيعيين فيما يتعلق بمعالجة البيانات الشخصية وتنقل هذه البيانات.
2016	دخول اللائحة العامة لحماية البيانات (GDPR) حيز التنفيذ.

المصدر: الباحثان

تعتبر الـ GDPR نقطة تحول في مجال حماية البيانات الشخصية، وقد أثرت بشكل كبير على صناعة الإعلانات الرقمية. ومع ذلك، لا تزال هناك تحديات كبيرة يجب مواجهتها في المستقبل. من المتوقع أن تستمر التشريعات المتعلقة بحماية البيانات في التطور والتغير، مما يتطلب من الشركات والمؤسسات التكيف مع هذه التغيرات والتأكد من امتثالهم للوائح الحالية والمستقبلية.

2. قانون كاليفورنيا لحماية خصوصية المستهلك (CCPA):

يمثل قانون كاليفورنيا لحماية خصوصية المستهلك (CCPA) خطوة مهمة في مجال حماية البيانات الشخصية¹⁵، خاصة في الولايات المتحدة، يهدف هذا القانون إلى منح سكان كاليفورنيا حقوقاً أكبر في التحكم ببياناتهم الشخصية، وتحديد كيفية استخدامها من قبل الشركات، وقد أحدث هذا القانون تغييرات جوهرية في صناعة الإعلانات الرقمية، مما دفع الشركات إلى إعادة النظر في ممارساتها المتعلقة بجمع البيانات واستخدامها.

أهم مبادئ CCPA :

- حق المعرفة: يمنح الأفراد الحق في معرفة البيانات الشخصية التي تجمعها الشركات عنهم، والأطراف الثالثة التي تشاركها هذه البيانات معها.
- حق الحذف: يمكن للأفراد طلب حذف بياناتهم الشخصية التي تجمعها الشركات.
- حق الانسحاب: يمكن للأفراد الانسحاب من بيع بياناتهم الشخصية.

الإشكالية القانونية حول الخصوصية الرقمية في مواجهة استهداف الإعلانات

- عدم التمييز: يحظر على الشركات التمييز ضد الأفراد الذين يمارسون حقوقهم بموجب القانون.

تأثير ال CCPA على صناعة الإعلانات الرقمية:

- تغيير نموذج الأعمال: أدى ال CCPA إلى تغيير جذري في نموذج الأعمال المعتمد على جمع البيانات واستهداف الإعلانات بشكل واسع.

- زيادة تكاليف الامتثال: فرض ال CCPA تكاليف كبيرة على الشركات، خاصة الشركات الكبرى، لتطوير أنظمة وتقنيات جديدة لضمان الامتثال.

- تركيز على الإعلانات السياقية: تحولت العديد من الشركات إلى الاعتماد على الإعلانات السياقية التي تعتمد على سياق البحث بدلاً من استهداف المستخدمين بناءً على بياناتهم الشخصية.

- تطوير تقنيات جديدة: أدى ال CCPA إلى تطوير تقنيات جديدة لحماية الخصوصية، مثل التشفير المتقدم والتعلم الآلي.

الجدول رقم 04: التسلسل الزمني لأهم التطورات التشريعية في كاليفورنيا

التاريخ	الحدث
2018	تم تمرير قانون كاليفورنيا لحماية خصوصية المستهلك (CCPA)
2020	بدأ تطبيق قانون CCPA بشكل كامل.

المصدر: الباحثان

وفيما يلي جدول مقارنة حول النصين القانونيين المذكورين أعلاه:

الجدول رقم 30: مقارنة بين ال CCPA وال GDPR

الميزة	ال CCPA	ال GDPR
النطاق الجغرافي	كاليفورنيا	الاتحاد الأوروبي بأكمله
الحقوق للممنوحة للأفراد	حقوق مشابهة لل GDPR	حقوق أكثر شمولية
العقوبات	غرامات مالية	غرامات مالية أكبر، وقد تصل إلى 4% من الإيرادات العالمية

التركيز	حماية المستهلكين	حماية البيانات الشخصية بشكل عام
---------	------------------	---------------------------------

المصدر: الباحثان

تواجه الـ CCPA تحديات في مواكبة التطورات التكنولوجية المستمرة، مثل الذكاء الاصطناعي وإنترنت الأشياء، كما أن هناك حاجة إلى تحقيق توازن بين حماية الخصوصية وتشجيع الابتكار في مجال التكنولوجيا، ويتطلب حماية البيانات في العصر الرقمي التعاون الدولي بين الدول لتطوير معايير مشتركة وحماية البيانات عبر الحدود.

2. قانون كندا لحماية المعلومات الشخصية وبيانات الكهرونية (PIPEDA)¹⁶:

يعد قانون حماية المعلومات الشخصية وبيانات الكهرونية (PIPEDA) في كندا من أبرز التشريعات التي تحكم جمع واستخدام البيانات الشخصية في القطاع الخاص. وقد تم تصميم هذا القانون لتوفير حماية شاملة لخصوصية الأفراد الكنديين، مع التركيز بشكل خاص على البيانات الشخصية التي يتم جمعها عن طريق الوسائل الإلكترونية، ومن مبادئه:

- الموافقة: يجب الحصول على موافقة صريحة من الأفراد قبل جمع واستخدام بياناتهم الشخصية، مع بعض الاستثناءات المحددة.

- الغرض المحدد: يجب أن يكون جمع واستخدام البيانات الشخصية لغرض محدد وواضح، ولا يجوز استخدامه لأغراض أخرى دون الحصول على موافقة جديدة.

- الدقة: يجب أن تكون البيانات الشخصية دقيقة وكاملة ومحدثة.

- الأمن: يجب على المنظمات اتخاذ جميع التدابير اللازمة لحماية البيانات الشخصية من الضياع أو السرقة أو الاستخدام غير المصرح به.

- الوصول: يحق للأفراد الوصول إلى بياناتهم الشخصية وتصحيحها.

تأثير PIPEDA على صناعة الإعلانات الرقمية

- تغيير نموذج الأعمال: أدى PIPEDA إلى تغيير جذري في نموذج الأعمال المعتمد على جمع البيانات واستهداف الإعلانات بشكل واسع.

الإشكالية القانونية حول الخصوصية الرقمية في مواجهة استهداف الإعلانات

- زيادة تكاليف الامتثال: فرض PIPEDA تكاليف كبيرة على الشركات، خاصة الشركات الكبرى، لتطوير أنظمة وتقنيات جديدة لضمان الامتثال.
 - تحديات في جمع البيانات: أصبح جمع البيانات واستخدامها لأغراض التسويق أكثر صعوبة، حيث يتعين على الشركات الحصول على موافقة صريحة من الأفراد.
 - تركيز على الإعلانات السياقية: تحولت العديد من الشركات إلى الاعتماد على الإعلانات السياقية التي تعتمد على سياق البحث بدلاً من استهداف المستخدمين بناءً على بياناتهم الشخصية.
 - تطوير تقنيات جديدة: أدى PIPEDA إلى تطوير تقنيات جديدة لحماية الخصوصية، مثل التشفير المتقدم والتعلم الآلي، ومن بين التحديات التي يواجهها هذا النص القانوني:
 - تطور التكنولوجيا: تواجه PIPEDA تحديات في مواكبة التطورات التكنولوجية المستمرة، مثل الذكاء الاصطناعي وإنترنت الأشياء.
 - التوازن بين الخصوصية والابتكار: هناك حاجة إلى تحقيق توازن بين حماية الخصوصية وتشجيع الابتكار في مجال التكنولوجيا.
 - التعاون الدولي: يتطلب حماية البيانات في العصر الرقمي التعاون الدولي بين الدول لتطوير معايير مشتركة وحماية البيانات عبر الحدود.
- أوجه التشابه بين التشريعات:
- الأهداف المشتركة: تهدف جميع التشريعات إلى حماية حقوق الأفراد في خصوصيتهم الرقمية وتنظيم جمع واستخدام البيانات الشخصية.
 - المبادئ الأساسية: تتشابه هذه التشريعات في العديد من المبادئ الأساسية، مثل:
 - الموافقة: يجب الحصول على موافقة صريحة من الأفراد قبل جمع ومعالجة بياناتهم الشخصية.
 - الشفافي، يجب أن تكون الشركات شفافة بشأن كيفية جمع البيانات واستخدامها.

- الحد من الأغراض: يجب أن يكون جمع البيانات واستخدامها مقصوداً على أغراض محددة وواضحة.
- أمن البيانات: يجب على الشركات اتخاذ جميع التدابير اللازمة لحماية البيانات الشخصية من أي انتهاكات.
- حقوق الأفراد: تمنح هذه التشريعات للأفراد مجموعة من الحقوق الأساسية، بما في ذلك الحق في الوصول إلى البيانات، وتصحيحها، وحذفها، والاعتراض على معالمتها.
- التأثير على صناعة الإعلانات: أدت جميع هذه التشريعات إلى تغييرات جوهرية في صناعة الإعلانات الرقمية، حيث أصبحت الشركات مضطرة إلى إعادة النظر في ممارساتها المتعلقة بجمع البيانات واستخدامها.
- أوجه الاختلاف بين التشريعات:
- نطاق التطبيق: تختلف التشريعات في نطاق تطبيقها، فهناك تشريعات ذات نطاق واسع تغطي جميع القطاعات، وتشريعات أخرى تركز على قطاعات معينة.
- مستوى الحماية: تختلف درجة الحماية التي توفرها هذه التشريعات للأفراد، فهناك تشريعات أكثر صرامة من غيرها.
- آليات التنفيذ: تختلف آليات تنفيذ هذه التشريعات، فبعضها يعتمد على الهيئات الرقابية المستقلة، بينما يعتمد البعض الآخر على الهيئات الحكومية القائمة.
- العقوبات: تختلف العقوبات المفروضة على المخالفين لهذه التشريعات، فبعضها يفرض غرامات مالية كبيرة، بينما يفرض البعض الآخر عقوبات جنائية.

الجدول رقم 05: الجدول المقارن

الميزة	قانون حماية البيانات الشخصية المصري	قانون تنظيم استخدام المعلومات المصري	GDPR	CCPA	PIPEDA

الإشكالية القانونية حول الخصوصية الرقمية في مواجهة استهداف الإعلانات

تاريخ الإصدار	2020	2018	2016	2018	2022
النطاق	واسع	واسع	الاتحاد الأوروبي	كندا	كندا
المبادئ الأساسية	موافقة، شفافية، حدود الأغراض، أمن البيانات، حقوق الأفراد	مشابهة لقانون حماية البيانات الشخصية	موافقة، شفافية، حدود الأغراض، أمن البيانات، حقوق الأفراد	موافقة، شفافية، حدود الأغراض، أمن البيانات، حقوق الأفراد	موافقة، الغرض المحدد، الدقة، الأمن، الوصول
التأثير على الإعلانات	تغييرات جوهرية	تغييرات جوهرية	تغييرات جوهرية	تغييرات جوهرية	تغييرات جوهرية

المصدر الباحثان

نتائج الدراسة:

بناءً على التحليل المقارن في هذه الدراسة، يمكن استخلاص النتائج التالية مع الأخذ بعين الاعتبار تطور الذكاء الاصطناعي وتأثيره على الإشكالية القانونية حول الخصوصية الرقمية في مواجهة استهداف الإعلانات:

أولاً: نتائج تتعلق بالتحديات والآثار:

- تزايد التهديدات على الخصوصية: يشكل استهداف الإعلانات تهديداً متزايداً على خصوصية الأفراد، حيث يتم جمع وتحليل كميات هائلة من البيانات الشخصية لتوجيه الإعلانات بشكل مخصص.
- تباين التشريعات: توجد فروقات كبيرة بين التشريعات العربية والغربية في مجال حماية البيانات، مما يخلق بيئة قانونية غير متجانسة.
- تطور سريع للتكنولوجيا: يتطور الذكاء الاصطناعي بسرعة كبيرة، مما يزيد من تعقيد المشكلة ويجعل من الصعب مواكبة التطورات التكنولوجية.
- تضارب المصالح: يتعارض الحق في الخصوصية مع المصالح الاقتصادية للشركات التي تعتمد على جمع البيانات وتحليلها.

- صعوبة في إنفاذ القوانين: تواجه السلطات صعوبة في إنفاذ القوانين المتعلقة بحماية الخصوصية في ظل التطور السريع للتكنولوجيا.
- نقص الوعي: يعاني الكثير من الأفراد من نقص في الوعي بحقوقهم في الخصوصية وكيفية حماية بياناتهم الشخصية.
- ثانياً: نتائج تتعلق بالتشريعات والقوانين:
 - الحاجة إلى تشريعات شامل: هناك حاجة إلى تشريعات شاملة وواضحة لحماية الخصوصية الرقمية.
 - أهمية المبادئ الأساسية: يجب أن تستند التشريعات إلى مبادئ أساسية مثل الموافقة والشفافية وحقوق الأفراد في الوصول إلى بياناتهم.
 - تحديات في تطبيق التشريعات: تواجه التشريعات الحالية تحديات في التطبيق، خاصة في ظل التطور السريع للتكنولوجيا.
 - الحاجة إلى آليات رقابة فعالة: يجب إنشاء آليات رقابة فعالة لضمان الامتثال للتشريعات.
- ثالثاً: نتائج تتعلق بالحلول والمقترحات:
 - التعاون الدولي: يجب تعزيز التعاون الدولي لوضع معايير مشتركة لحماية البيانات.
 - توعية الأفراد: يجب توعية الأفراد بحقوقهم في الخصوصية وكيفية حماية بياناتهم الشخصية.
 - تطوير التقنيات: يجب تطوير تقنيات جديدة لحماية الخصوصية، مثل التشفير المتقدم والتعلم الآلي.
 - تعديل التشريعات: يجب مراجعة وتحديث التشريعات القائمة لمواكبة التطورات التكنولوجية.

- التوازن بين الخصوصية والابتكار: يجب تحقيق توازن بين حماية الخصوصية وتشجيع الابتكار في مجال التكنولوجيا.

مناقشة النتائج:

فيما يتعلق بالتحديات والآثار: تؤكد الدراسة على التهديد المتزايد للخصوصية الرقمية نتيجة لتطور تقنيات استهداف الإعلانات التي تعتمد على جمع وتحليل كميات هائلة من البيانات الشخصية. هذا التطور يفرض تحديات كبيرة على صعيد حماية الخصوصية، خاصة مع تباين التشريعات بين الدول وتطور التكنولوجيا بشكل أسرع من قدرة التشريعات على مواكبته. كما أن الصراع بين الحق في الخصوصية والمصالح الاقتصادية للشركات التي تعتمد على البيانات يزيد من تعقيد المشكلة.

فيما يتعلق بالتشريعات والقوانين: تظهر الدراسة الحاجة الملحة إلى تشريعات شاملة وواضحة لحماية الخصوصية الرقمية، مع التركيز على مبادئ أساسية كالموافقة والشفافية وحقوق الأفراد في الوصول إلى بياناتهم. ومع ذلك، تواجه هذه التشريعات تحديات في التطبيق، خاصة في ظل التطور السريع للتكنولوجيا. كما تسلط الدراسة الضوء على أهمية آليات الرقابة الفعالة لضمان الامتثال لهذه التشريعات.

فيما يتعلق بالحلول والمقترحات: تقدم الدراسة مجموعة من الحلول والمقترحات للتعامل مع هذه التحديات، بما في ذلك تعزيز التعاون الدولي لوضع معايير مشتركة لحماية البيانات، وتوعية الأفراد بحقوقهم، وتطوير تقنيات جديدة لحماية الخصوصية، وتعديل التشريعات القائمة لمواكبة التطورات التكنولوجية. كما تؤكد الدراسة على أهمية تحقيق التوازن بين حماية الخصوصية وتشجيع الابتكار في مجال التكنولوجيا.

توصيات الدراسة:

- ضرورة وضع تشريعات وطنية ودولية شاملة تغطي جميع جوانب حماية الخصوصية الرقمية، مع مراعاة التطورات التكنولوجية المتسارعة.

- يجب أن تشمل هذه التشريعات تعريفات واضحة للبيانات الشخصية وأنواع المعالجة، وحقوق الأفراد، وواجبات المشغلين، وآليات الرقابة والعقوبات.
- يجب أن تكون الموافقة على جمع واستخدام البيانات الشخصية صريحة وواضحة، وأن يتم الحصول عليها بطريقة شفافة.
- يجب توفير خيارات واضحة للمستخدمين لقبول أو رفض جمع واستخدام بياناتهم.
- يجب على الشركات أن تكون شفافة بشأن كيفية جمعها واستخدامها للبيانات الشخصية.
- يجب أن توفر معلومات واضحة وموجزة للمستخدمين حول كيفية استخدام بياناتهم.
- يجب تقييد جمع البيانات الشخصية إلى الحد الأدنى الضروري لتحقيق الأغراض المعلنة.
- يجب ضمان حقوق الأفراد في الوصول إلى بياناتهم الشخصية وتصحيحها وحذفها.
- يجب منح الأفراد الحق في الاعتراض على معالجة بياناتهم الشخصية لأغراض التسويق المباشر.
- يجب إنشاء هيئات مستقلة للرقابة على تطبيق قوانين حماية البيانات، مع منحها صلاحيات واسعة للتحقيق في الشكاوى واتخاذ الإجراءات اللازمة.
- يجب فرض عقوبات رادعة على المخالفين لهذه القوانين.
- يجب تعزيز التعاون الدولي لوضع معايير مشتركة لحماية البيانات وتسهيل تبادل المعلومات بين الدول.
- يجب إنشاء آليات للتعاون بين الهيئات الرقابية في مختلف الدول.
- يجب بذل جهود كبيرة لتوعية الأفراد بحقوقهم في الخصوصية وكيفية حماية بياناتهم الشخصية.

- يجب تشجيع البحث والتطوير في مجال تقنيات حماية الخصوصية، مثل التشفير والتعلم الآلي.

- يجب تطوير أدوات تمكن الأفراد من التحكم في بياناتهم الشخصية.

- يجب تحقيق توازن بين حماية الخصوصية وتشجيع الابتكار في مجال التكنولوجيا.

- يجب أن يكون الابتكار التكنولوجي خاضعًا لضوابط قانونية لحماية الخصوصية.

خاتمة:

تُعتبر حماية الخصوصية الرقمية تحديًا معقدًا ومتشابكًا في ظل التطور المتسارع للتكنولوجيا الرقمية وانتشار ممارسات استهداف الإعلانات، لقد أظهرت هذه الدراسة أن التباين الكبير في التشريعات بين الدول، والتطور السريع للذكاء الاصطناعي، وصراع المصالح بين حماية الخصوصية والمصالح الاقتصادية للشركات، كلها عوامل تساهم في تعقيد هذه المسألة، ومع ذلك، فإن دراسة الإشكاليات القانونية تفتح آفاقًا جديدة لحماية الخصوصية الرقمية من خلال اقتراح مجموعة من الحلول والمقترحات، فالتعاون الدولي وتطوير تشريعات شاملة وواضحة، إلى جانب توعية الأفراد وتعزيز آليات الرقابة، هي خطوات حاسمة نحو بناء مستقبل رقمي يحترم خصوصية الأفراد، إن تحقيق التوازن بين حماية الخصوصية وتشجيع الابتكار التكنولوجي يمثل تحديًا كبيرًا، يجب أن يكون الابتكار خاضعًا لضوابط قانونية تحمي حقوق الأفراد في الخصوصية، كما يجب أن يكون هناك استثمار مستمر في البحث والتطوير لتطوير تقنيات تحمي الخصوصية، في النهاية، فإن حماية الخصوصية الرقمية هي مسؤولية مشتركة تقع على عاتق الحكومات والشركات والمجتمع المدني والأفراد، من خلال العمل معًا، يمكننا بناء مستقبل رقمي آمن يحمي حقوق الأفراد في الخصوصية ويضمن في الوقت نفسه الاستفادة من التقدم التكنولوجي.

المراجع:

¹ Benedetta Taddei, Giovanni Vespoli, Lisa de Luca, Enrico Imbimbo, The concept of privacy in the digital world according to teenagers, *Journal of Public Health*, (2024), p11.

² James C. Rice, Fiona Sussan, Digital Privacy: A Conceptual Framework for Business, *Journal of Payments Strategy & Systems*, 10 (3), (2016), pp260-266.

³ ico.org.uk, Your right to get your data deleted, acces 25-09-2024: <https://ico.org.uk/for-the-public/your-right-to-get-your-data-deleted/>

⁴ Shafi Goldwasser, Sanjam Garg, Formalizing Data Deletion in the Context of the Right to Be Forgotten, In book: *Advances in Cryptology – EUROCRYPT*, (2020), pp.373-402.

⁵ Philippe Jougleux, Identity theft and internet, *International Journal of Liability and Scientific Enquiry*, 5(1), (20212), pp37 – 45.

⁶ Sherzod Raimberdiyev, Said Gulyamov, Personal Data Protection as a Tool to Fight Cyber Corruption, *International Journal of Law and Policy*, 1(7), (2023), p11.

⁷ Nkechi Emmanuella Eneh, Oluwatosin Reis, Anthony Anyanwu, Benedicta Ehimuan, PRIVACY LAW CHALLENGES IN THE DIGITAL AGE: A GLOBAL REVIEW OF LEGISLATION AND ENFORCEMENT, *International Journal of Applied Research in Social Sciences*, 6(1), (2024), 73-88.

⁸ Kotch Obudho, The Impact of Data Privacy Laws on Digital Marketing Practices, *Journal of Modern Law and Policy*, 4(1), (2024), 35-48.

⁹ الجريدة الرسمية للجمهورية العربية المصرية، قانون رقم 151 لسنة 2020 المتعلق بحماية البيانات الخصوصية، العدد 28 مكرر، 2020-07-15، ص2.

¹⁰ الجريدة الرسمية للجمهورية العربية المصرية، القانون رقم 175 لسنة 2018 المتعلق بمكافحة جرائم تقنية المعلومات العدد 32 مكرر، ص3، تاريخ التصفح 2024-09-25

<https://cairo52.docdroid.com/S70ROL9/175-lsn-2018-pdf>

¹¹-25 هيئة الخبراء بمجلس الوزراء، نظام حماية البيانات الشخصية 2021، تاريخ التصفح :2024-09 <https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/b7cfae89-828e-4994-b167-adaa00e37188/1>

¹² Gdpr, General Data Protection Regulation, (2016), acces 19-09-2024: <https://gdpr-info.eu/>

¹³ Mistale Taylor, Cedric Ryngaert, The GDPR as Global Data Protection Regulation?, AJIL Unbound, 114, (2020), p5-9

¹⁴ Abdulah M. Aseri, The Implication of the European Union's General Data Protection Regulation (GDPR) on the Global Data Privacy, Journal of Theoretical and Applied Information Technology, Vol.98, No 04, (2020), pp 696-697.

¹⁵ Jeeyun Sophia Baik, Data privacy against innovation or against discrimination?: The case of the California Consumer Privacy Act (CCPA), Telematics and Informatics, 52, (2022), p07.

¹⁶ priv.gc.ca, The Personal Information Protection and Electronic Documents Act (PIPEDA), acces 15-09-2024, Date modified 2021-12-08, <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/>