



مجلة ألف: اللغة، الإعلام والمجتمع، مصنفة في فئة ب

بوسجرة ليلىا - المدرسة الوطنية العليا للصحافة وعلوم الاعلام وبودربالة عبد القادر - جامعة قاصدي
مرباج، ورقلة

آليات حماية خصوصية البيانات في عصر الميتافيرس: المتداول والضروري

Mécanismes de protection des particularités des données à l'ère du Métaverse : Ce qui est en vigueur et le nécessaire

Data Peculiarities Protection Mechanisms in the Age of Metaverse: What is Effective and what is Necessary

تاريخ النشر ASJP	تاريخ الإلكتروني	تاريخ الإرسال	
-2023 05-25	2023-05-15	2023-03-15	

الناشر: Edile- Edition et diffusion de l'écrit scientifique

إيداع قانوني: 2014-6109

النسخة الورقية: 2023 05-25

<https://www.asjp.cerist.dz/en/PresentationRevue/226>

ترقيم الصفحات: 351-363

دمد-د: 2437-0274

النشر الإلكتروني: <https://aleph.edinum.org>

تاريخ النشر: 2023-05-15

ردمد-د: 2437 1076-

المرجعية على ورقة

بوسجرة ليلىا وبودربالة عبد القادر، « آليات حماية خصوصية البيانات في عصر الميتافيرس: المتداول والضروري»، Aleph, 10 (3) | 2023, 351-363.

المرجع الإلكتروني

بوسجرة ليلىا وبودربالة عبد القادر، « آليات حماية خصوصية البيانات في عصر الميتافيرس: المتداول والضروري»، Aleph [En ligne], | 2023 URL : <https://aleph.edinum.org/8793>

آليات حماية خصوصية البيانات في عصر الميتافيرس: المتداول والضروري

Mécanismes de protection des particularités des données à l'ère du Métaverse : Ce qui est en vigueur et le nécessaire

Data Peculiarities Protection Mechanisms in the Age of Metaverse: What is Effective and what is Necessary

بوسجرة ليليا - المدرسة الوطنية العليا للصحافة وعلوم الإعلام
بوردباله عبد القادر - جامعة قاصدي مرياح، ورقلة

مقدمة

دأبت العديد من الشركات إلى تخصيص العديد من المخصصات المالية والكوادر البشرية ضمن مشروع الميتافيرس رغم أنه لم يتجسد بالكامل، عبر الدعوة إلى بناء مستقبل يتيح للناس المزيد من وسائل العمل واللعب والتواصل، ومع ذلك يثير الميتافيرس العديد من الهواجس فيما يتعلق بحماية البيانات الشخصية، فمن خلال تقديم هذا المشروع كواقع افتراضي مع صور رمزية يتحكم فيها المستخدم، من المحتمل أن تؤدي هذه التكنولوجيا الجديدة إلى ولادة فئات جديدة من البيانات الشخصية بالإضافة إلى زيادة كمية البيانات التي يتم تجميعها، ومع ذلك لنا أن نتساءل هل هذه البيانات شخصية حقا؟ ويمكننا الإجابة أنه في عالم الميتافيرس يتم تمثيل المستخدم بواسطة صورة رمزية تشكل نسخة مطابقة عن الشخص المستخدم لهذا العالم عبر بيئته الحيوية والسلوكية، لذلك ليس هناك شك في أن البيانات المقدمة والمجمعة يمكن إرجاعها إلى المستخدمين المعنيين وبالتالي فهي بيانات شخصية.

أبعد من ذلك، يبدو أن هذه البيانات ستساعد على فهم عمليات تفكير العملاء بشكل أفضل، إذ تتيح تطبيقات ومواقع الهاتف المحمول اليوم للمؤسسات فهم كيفية تحرك الأشخاص عبر الإنترنت أو من خلال أحد التطبيقات، بينما سيتيح استخدام الميتافيرس إمكانية متابعة الأفراد بطريقة أكثر حميمية من خلال الكم الغير مسبوق من البيانات المجمعة مثل تعبيرات الوجه أو الإيماءات أو أنواع أخرى من ردود الفعل التي قد تنتجها الصورة الرمزية أثناء تفاعلها وبالتالي ستتيح هذه المعلومات للمؤسسات فهم سلوك المستخدم بشكل أفضل وتكييف الحملات الاشهارية بطريقة هادفة للغاية، وهو ما يطرح بالحاح العديد من التساؤلات حول: ما هي آليات حماية خصوصية البيانات في عصر الميتافيرس بين ما هو متداول من لوائح وقوانين وما هو ضروري لمواكبة هذا الفضاء الجديد؟

1. البيانات الشخصية، مفتاح الاستهداف المباشر للمؤسسات

تثير مسألة أمن المعلومات وحماية خصوصية بيانات المستخدمين قلق المتخصصين في أمن الشبكات كما يحذرون من البيانات الحساسة التي يمكن للمؤسسات تجميعها واستثمارها على المدى الطويل، ففي منطلق الاستخدام عبر الشبكات تتم عملية تجميع البيانات أولا لضمان « تجربة المستخدم » ولكن بمجرد تجميعها تصبح تلك المعلومات تهديدا كبيرا لإمكانية إساءة استخدامها، ويشير خبير الأمن السيبراني Axel Legay في هذا الصدد أنه بالإضافة إلى خطر تسريب البيانات المصرفية مثلا، تبرز أخطار أخرى مرتبطة بسلوك اللاعبين عبر الألعاب في الواقع الافتراضي أين تتيح عملية نقل المستخدم في هذا الكون الخيالي وتفاعله مع أناس حقيقيين آخرين عبر تقنيات الذكاء الاصطناعي جمع الكثير من الأحداث والحركات التي تسجلها أجهزة الاستشعار ووحدات التحكم وخوذة الواقع الافتراضي الخاصة به، في هذه الحالة مثلا، يمكن للاعب الذي يميل إلى مهاجمة أعدائه الافتراضيين أن يقدم ملفا شخصيا مثيرا للاهتمام للبنوك في الحياة الواقعية، فقيامه بالمخاطرة الكبيرة يسمح لها استخدام ذلك لتشجيعه على الحصول على قرض بسعر متغير بناء على الصورة المقارنة للملامح شخصيته ومميزاتها (Legay, 2022).

2. الحركات والمعلومات الحساسة

صرح Jeremy Bailenson في مقال نشره حول القياسات الحيوية المرتبطة بالشخصية سنة 2018 تحت عنوان: «20 minutes passées dans une simulation en VR permet un peu moins de 2 millions de mouvements du corps من الوصول إلى مجموع بيانات بهذا الحجم في عدة عقود من دراسة السلوك الغير لفظي (Boilenson, 2018)، بينما يشير Axel Legay أنه بعد مرور 20 دقيقة من ولوج المستخدم يمكن للمحللين التنبؤ بما سيحدث طيبيا وسلوكيا من خلال البصمة الإلكترونية المنتجة له، ويتابع قائلاً أنه من خلال ملاحظة الصورة الرمزية للمستخدم Avatar يمكن تحديد هوية المستخدم حتى ولو كان مجهولا على الميتافيرس.

وخلصت دراسة لمجلة Nature نشرت في أكتوبر 2020 إلى أن تتبع بيانات الواقع الافتراضي، ووضعية الجسم، والحركات يعد مصدرا قويا جدا للمعلومات من خلال إنشاء روابط بين حركات معينة للجسم والإبداع والتعلم والسمات السلوكية الأخرى، إضافة إلى إمكانية ربط السلوكات المسجلة في بيانات التتبع باضطرابات طبية مثل اضطرابات الانتباه أو التوحد أو إجهاد ما بعد الصدمة.

وبنفس الطريقة التي يتم بها تتبع تنقلاتنا على الإنترنت لتزويدنا بإعلانات مستهدفة، يمكن لهذه الأكوان الافتراضية أيضا تكييف لوحاتها الإعلانية وفقا لكل مستخدم حيث يمكننا الرجوع إلى المعلومات وتحديد أن الشخص مريض وتقديم الدواء على سبيل المثال.

3. أمن معدات الإبحار

من جهة أخرى يثير احتكار شركات التكنولوجيا لدول بعينها إنتاج المعدات الخاصة بالولوج إلى هذا الفضاء الجديد مخاوف أخرى مرتبطة بإمكانية تجميع المعلومات وتتبع الأفراد، حيث يشير Axel Legay إلى أن اعتبار غالبية معدات الإبحار مصنعة في آسيا يطرح مخاوف احتواءها على شرائح خاصة بتجميع المعلومات عن المستخدمين، وبالتالي قد لا تساعد لوائح حماية البيانات مثل اللائحة الأوروبية العامة لحماية البيانات في ضمان أكبر قدر من الحماية للمستخدمين في أوروبا يقول Axel Legay، والأمر أخطر بالنسبة للدول التي لا تعتمد مثل هذه اللوائح ومنها الدول العربية، وعلى قدر ما تبدو عملية جمع البيانات آمنة غير أن هامش الأمن هذا قد يقل في حالة استخدام معدات غير آمنة، وهو هامش غير مضمون أيضا في ظل زيادة التبعية التكنولوجية وعدم توافق ما هو موجود من لوائح مع التقنية ذاتها، ناهيك على أنه إذا كانت اللوائح مقيدة فإن بعض الشركات تعمل على تطوير آليات معينة للتحايل على تلك اللوائح والقيود (Legay, 2022).

4. خصوصية البيانات في البيئة الافتراضية: تعقيدات الميتافيرس

تدعم البيانات في عالم الواقع الافتراضي الميتافيرس النظام البيئي الخاص به، حيث يعتمد على جمع بيانات المستخدم في الوقت الفعلي (سلوك المستخدم، تفضيلاته والاستجابات الفسيولوجية...) لتمكين هذه التجربة الجديدة، اعتبارا أن الميتافيرس يسعى إلى إنشاء هذا العالم الرقمي الفريد من نوعه أو التجربة الافتراضية أين ستكون معالجة بيانات المستخدم في المقدمة لتسهيل تجربة سلسلة، ومع انتشار قدرات معالجة الجيل الخامس 5G وتقنيات إنترنت الأشياء يمكن التوقع بتجميع كم هائل من البيانات عن بيئة الفرد خصوصا مع طبيعة البيئة الخاصة للميتافيرس (كما يوضحه الشكل رقم 1 أدناه)، إلا أن مع تخلف القوانين ومحاولة اللحاق بالتطور التكنولوجي الحاصل قد يحتاج مفهوم حماية البيانات بالكامل إلى إعادة التفكير في سياق بيئة الميتافيرس الجديدة (Ball, 2022).

الشكل 1: ركائز بيئة الميتافيرس



المصدر: <https://www.wavestone.com/fr/insight/fondamentaux-metaverse-differents-ecosystemes>

5. إعادة تحديد مفهوم حماية البيانات في بيئة الميتافيرس

يهدف المفهوم الواسع للميتافيرس إلى دمج حدود العالمين المادي والرقمي من خلال جمع البيانات ومعالجتها على مستوى دقيق للغاية، ولا تعتمد هذه التقنيات فقط على البيانات الملموسة « سواء كانت شخصية أم لا » والتي يغذيها المستخدمون، ولكن أيضا على البيئة وردود الفعل والاستجابات والمنبثبات والمؤشرات الفسيولوجية الأخرى للمستخدمين والتي قد لا تكون مرئية حتى للمستخدم نفسه في الوقت الحالي، وفي حين أن أمور مثل تحديد سمات المستخدم والإعلانات المستهدفة شائعة فإن تصنيف المستخدم يحتوي على بيانات أقل تدخلا مثل وقت مشاهدة المحتوى الرقمي، والإعجابات وعدم الإعجاب، والعمر، والجنس، والاسم والنشاط على منصات الوسائط الاجتماعية كما يمكن للفاعلين تتبع أنماط السلوك لإنشاء ملفات تعريف المستخدمين، غير أن نطاق التنميط هذا يمكن أن يتضاعف في بيئة الميتافيرس مع الأشكال الجديدة للبيانات الشخصية التي يتم جمعها والذي سيؤدي إلى اندماج غير مسبوق بين بيانات الأفراد والتكنولوجيا، والتي ستشمل طرقا جديدة للحصول على معلومات ملف تعريف المستخدم مثل القزحية وحركات الوجه وتتبع الاستجابة الصوتية (Berendes, 2022).

جانب آخر مثير للاهتمام هو إنشاء « الصور الرمزية Avatar » على الميتافيرس وتنميط هذه الصور الرمزية والتي يمكن أن يكشف تحليل نشاط الصورة الرمزية للمستخدم أيضا عن معلومات مهمة حول سلوك المستخدم، نتيجة لذلك، سيصبح تحديد مواصفات المستخدم أكثر دقة، كما سيؤدي هذا بالتأكيد إلى فتح طرق جديدة للشركات مع زيادة اعتماد الخدمات القائمة على الميتافيرس، وسيتم جمع هذه الأشكال الجديدة من البيانات ومعالجتها في الوقت الفعلي باستخدام الآلات الذكية ومعدات الواقع المختلط (الواقع الافتراضي والواقع المعزز).

وعليه تؤدي خصوصية هذه البيئة الجديدة إلى ظهور أنواع جديدة من البيانات الشخصية التي تعتمد الهيئات والمؤسسات إلى تجميعها بطرق لم يسبق لها مثيل وإضافة أبعاد جديدة لتنظيم البيانات الشخصية وغير الشخصية، وبالتالي سيكون ضمان خصوصية المستخدم أمرا بالغ الأهمية والتعقيد في بيئة يصبح فيها تتبع المستخدم وتنميته أمرا سهلا للغاية.

مع الاهتمام المتزايد الذي اكتسبته بيئة الميتافيرس خلال الأشهر القليلة الماضية، ومع نوع مشاركة الفاعلين الكبار وتدفق رؤوس الأموال في مشاريع الميتافيرس، فمن الممكن تماما أن ينجذب مجرمو الإنترنت إلى هذا الفضاء، وبالتالي قد تكون البيانات الشخصية للأفراد والسلع الافتراضية والصور الرمزية وغيرها من أصول الميتافيرس معرضة للخطر بسبب

مجرمي التعريف، كما تصبح المشكلة أكثر تعقيدا لأنه يمكن تخزين بيانات الميتافيرس على ميتافيرس لامركزي، نظرا لعدم وضوح تنظيم الأنظمة القائمة على Blockchain (والتي قد تكون موجودة خارج حدود الدولة)، ويصبح تنفيذ اللوائح القانونية تحديا في حد ذاته.

بالإضافة إلى الآثار الخطيرة للأمن السيبراني، ستكون هناك أيضا مجالات مهمة للرقابة في مجال الملكية الفكرية (مثل قضايا حقوق التأليف والنشر مع الصور الرمزية) والإنفاذ من قبل السلطات القانونية أو التنظيمية، سيتعين على النظام القانوني ككل (بما في ذلك القوانين الجنائية) التكيف مع التحديات الفريدة والجديدة التي يطرحها الميتافيرس.

مع تزايد عدد المستخدمين النشطين شهريا ضمن منصات Meta، فإن ضمان عدم إضعاف ممارسات الأمن السيبراني وحقوق المستخدمين (فيما يتعلق ببياناتهم الشخصية) تعتبر مهمة شاقة فيما يتعلق بالاستقرار الهائل للبيانات وممارسات جمع البيانات المتطفلة وتحليل البيانات واسعة النطاق التي قد تولد أضرارا وتهديدات محتملة جديدة والذي يجب أن يواكبه تأطير قانوني ملائم لدرأ هذه المخاطر، بيدومهما هنا الإشارة إلى أن المعضلة تتعزز من خلال القيود المفروضة على نقل البيانات عبر الحدود بموجب القوانين المحلية على حماية البيانات بسبب اعتماد الميتافيرس على التدفق الحر للمعلومات بين المنصات وحدود العالم المادي.

6. النظام الحالي لنقل البيانات عبر الحدود ومسألة توطين البيانات

إعتبارا أن الميتافيرس يسعى إلى سد الفجوة بين الحقيقي والافتراضي يتطلب ذلك تبادلا سلسا للبيانات بين الأنظمة الأساسية المختلفة وعبر الحدود، فعلى سبيل المثال سيتمكن المستخدمون فعليا من زيارة المتاجر الافتراضية الموجودة في الخارج واكتشافها والتعامل معها عبر أجهزة الواقع الافتراضي أو الواقع المعزز، وهذا ما من شأنه أن يؤدي إلى نقل معلومات المستخدم (بما في ذلك بيانات الدفع، ردود الفعل الفسيولوجية في الوقت الحقيقي، البيانات السلوكية، المعارف الشخصية)، يمكن أيضا إجراء المعاملات في الميتافيرس من خلال العملات المشفرة والأصول الرقمية الافتراضية، بالإضافة إلى ذلك وحرصا على ضمان سهولة الوصول على نطاق عالمي، من المفترض أن النظام البيئي للميتافيرس بأكمله يمكن أن يعمل على Blockchain، وبالتالي، يمكن تخزين البيانات على أجهزة الكمبيوتر والعقد الموجودة في جميع أنحاء العالم (بغض النظر عن الحدود الوطنية)، نظرا لأنه قد يتم تخزين بيانات Blockchain على عقد موجودة خارج الدولة، فسيكون من المستحيل تقريبا توقع امتثال الكيانات التي تتحكم في تلك البيانات لمتطلبات توطين البيانات.

يشير المختصون إلى أنه يمكن للحكومة إنشاء استثناء لتوطين البيانات لضمان التوافق مع النماذج المستندة إلى Blockchain، غير أن متطلبات توطين البيانات في ولايات قضائية متعددة مثل الهند والصين والاتحاد الأوروبي يمكن أن تؤدي بالفعل إلى خلق حواجز أمام تدفقات البيانات عبر الحدود، لذلك من الضروري إعادة التفكير لإيجاد توازن بين تسهيل تدفق البيانات عبر الحدود وحماية المصالح الوطنية وهو أمر لم توفق الدول العربية في المطالبة به أو تأطيره ضمن إطار بيئي جامع لحد الآن (Abhinov Chandan, 2021).

نشير هنا إلى أن حكم (Schrems II (2020) الأخير في الاتحاد الأوروبي، والذي ألغى درع الخصوصية بين الاتحاد الأوروبي والولايات المتحدة الأمريكية مهد بشكل فعال الطریق لتوطين البيانات، فوفقاً لهذا الحكم، لا يمكن نقل البيانات المحمية بموجب اللائحة العامة لحماية البيانات إلى الخارج إلا إذا تم استيفاء بعض الشروط الصارمة، الأمر الذي قد يكون له تداعيات خطيرة على قطاع التعهيد، مما قد يضر بالشركات الأوروبية وغيرها، وبالتالي سيصبح التدفق الحر للبيانات ضرورياً لضمان عدم تقييد الاتصالات والمعاملات عبر الحدود في الميتافيرس أو تأخيرها بسبب معايير التخزين المحلية أو التصاريح الإضافية المطلوبة لمثل هذا التبادل، فمن الضروري التحديد أو التعرف على أنواع البيانات الشخصية التي لا تنطبق عليها قيود موقع البيانات، وبالتالي يمكن أن يغذي الميتافيرس النقاش المستمر بين توطين البيانات والتدفق الحر للبيانات وسيكون من المثير للاهتمام معرفة ما إذا كانت المصالح الوطنية ستسود على العولمة، وفي حالة عدم وجود إطار شامل لتبادل البيانات الشخصية عبر الحدود واستخدام معلومات ملف تعريف المستخدم، قد يجتمع أصحاب المصلحة، بما في ذلك المطورون والمنظمات والهيئات الصناعية، للاتفاق على إطار تنظيمي ذاتي لضمان حماية البيانات الشخصية في الميتافيرس وتسهيل التدفق الحر للبيانات، في الوقت نفسه يمكن لإطار تنظيمي تمكيني أن يعطي الصناعة دفعة قوية.

7. لوائح الملكية الفكرية والميتافيرس

يثير الميتافيرس قضية رئيسية أخرى هي تلك المتعلقة بحقوق التأليف والنشر وحقوق الملكية الفكرية لمبدعي الميتافيرس، فتصميمه ثوري لا أحد يجادل فيه لذلك توجد ثغرات قانونية مرتقبة مرة أخرى، حيث من المحتمل أن يشارك المستخدمون أنفسهم في إنشاء المحتوى، فما ينشأ في الحياة الواقعية، سوف يخلق في الحياة الافتراضية، لذلك سوف تطفو قضايا حقوق التأليف والنشر من خلال تخيل ما يمكن أن يكون عليه الميتافيرس، من الواضح أن التشريع الحالي وخاصة البنى التحتية الإدارية الخاصة به من خلال وسيط الإدارات المرجعية لن يكون قادراً على جمع هذا الكم الهائل من الأعمال التي يتم إنشاؤها في كل لحظة.

ومنه يجب تأطير شروط تطبيق واستغلال الحقوق المرتبطة بهذه الأعمال الفكرية من وجهة نظر قانونية بشكل مستمر، الشروط العامة للاستخدام أو الشروط العامة للبيع أو حتى العقود الافتراضية للتفاعلات المختلفة بين الجهات الفاعلة في الميتافيرس ورغم أنه هناك العديد من الدلائل حول هذه النقطة غير أنها تبقى في الوقت الحالي نظرية بحتة، باختصار يفرض الميتافيرس ضرورة أن يواكب المشرعون ورجال القانون هذه الابتكارات وأن يكونوا في طليعتها.

8. التنظيم القانوني للميتافيرس

من الناحية القانونية دائما، يثير هذا العالم البديل العديد من النقاشات والتأملات المختلفة، وإحدى القضايا الرئيسية هي تلك المتعلقة بإدارة البيانات الشخصية المتعلقة بالميتافيرس، بعض الإجابات موجودة بالفعل في بعض اللوائح الدولية الحالية ومنها بالأساس اللائحة الأوروبية العامة لحماية البيانات (GDPR) والتي أسس من خلالها المشرع الأوروبي للضوابط المتعلقة بحماية البيانات الشخصية، (ويوضح الشكل أدناه أطر إرساء اللائحة الأوروبية العامة لحماية البيانات والتي تخضع لها كل مؤسسة في العالم تعمل على معالجة البيانات الشخصية للمستخدمين الأوروبيين).

الشكل رقم 2: يوضح أطر إرساء اللائحة الأوروبية العامة لحماية البيانات



المصدر: <https://koesio.com/comprenez-les-enjeux-du-rgpd>

تتيح اللائحة الأوروبية العامة لحماية البيانات فهم أسئلة معينة خاصة بالميتافيرس بشكل صحيح، ففي الواقع أتاح التنسيق الأوروبي إمكانية إثبات أن اللائحة العامة لحماية البيانات تنطبق على أي معالجة للبيانات الشخصية تتم في إطار عرض الخدمة المقدم للأشخاص المقيمين داخل الاتحاد الأوروبي، لذلك يمكن القول بأن اللائحة العامة لحماية البيانات قابلة للتطبيق على الميتافيرس داخل أوروبا، قد يبدو هذا غير بديهي لأن الميتافيرس يبدو بلا حدود، إنه بطبيعته « غير واقعي »، ومع ذلك يبدو أنه من المستحيل أن يتعلق الأمر بمكان ثابت إقليميا دون الخضوع للوائحها، بنفس طريقة العملات المشفرة سيجير المستخدمون المقيمون لهذه التقنيات على احترام الإطار التنظيمي لدولهم، وبالتالي سيتعين

على الفاعلين « المبدعين » في الميتافيرس أيضا الامتثال لهذه اللوائح إذا كانوا يريدون رؤية أدواتهم قابلة للتطبيق على هؤلاء السكان، سيواجه المضيفون والناشرون ومقدمو الخدمات المشاركون في تطوير هذا العالم الافتراضي تعقيدا قانونيا قويا للغاية، إذ غالبا ما تختلف تشريعات الدولة اختلافا عميقا بشأن هذه القضايا، وبالتالي يبدو أن الاتحاد الأوروبي من خلال تنسيقه التشريعي، يمثل أرضية مواتية جدا لهؤلاء الفاعلين المؤسسين للميتافيرس، وإذا كان من الممكن نظريا تطبيق اللوائح الحالية بالفعل على للميتافيرس، فمن المحتمل أن يجبر تعقيد البيانات المتصورة لميتافيرس المستقبلي (الأحاسيس، والسلوكيات، والقدرات...) المشرع على إتمام عمله.

الشكل رقم 3 : أسس انشاء توثيق لمختلف الإجراءات المبررة للتطبيق الصحيح



التحديد: تحديد البيانات والاستخدامات المرتبطة بالبيانات الشخصية



الحماية: وضع آليات للحماية الضرورية وضمان الواجب الاعلامي والحق في النسيان



المرجع: يجب على كل مؤسسة تضم أكثر من 250 متعامل تعيين مسؤول حماية البيانات



التوعية: إعلام و تدريب المتعاملين حول تحديات البيانات الشخصية

المصدر: <https://koesio.com/comprenez-les-enjeux-du-rgpd>

يمثل قانون حماية البيانات الهندي (DPB) من جهته تبعا لللائحة العامة الأوروبية لحماية البيانات (GDPR) من أجل تنظيم مجال البيانات الشخصية الحساسا اقتصاديا واستراتيجيا، ولا يشكل استثناء من حيث أن الهيكل والتوجه العام لتنظيم الجهات الفاعلة فيما يتعلق بمعالجتها للبيانات الشخصية لهما العديد من أوجه التشابه مع محتوى اللائحة العامة الأوروبية لحماية البيانات، وبالتالي يحدد مجلس إدارة البيانات (DPB) التزامات « المؤتمنين في البيانات » (مفهوم مكافئ لمراقب البيانات) في النسخة الأوروبية، الذين يجب أن يحصلوا على موافقة الأشخاص الذين تنتهي إليهم البيانات الشخصية إذا كانوا يريدون أن يكونوا قادرين على معالجتها. تتعلق الالتزامات المحددة الأخرى بـ « معالجي البيانات » (مؤهل معادل للمقاول من الباطن في اللائحة العامة الأوروبية لحماية البيانات)، سواء كان الأمر يتعلق بالشروط التي يجب بموجبها الحصول على الموافقة (والتي يجب أن تكون حرة ومحددة وواضحة)، ونطاق اللوائح (التي تكون ذات صلة عندما يتعلق الأمر ببيانات المواطنين في الهند)، ومبدأ التقليل، والحقوق بالنسبة للأشخاص المعنيين أو القواعد

الخاصة ببيانات القاصرين، فإن تنفيذ قانون الإجراءات الجنائية مشابه في العديد من الجوانب للقانون العام لحماية البيانات الأوروبي (GDPR) (Faucomprez, 2022). مع ذلك، فقد تم إدخال اختلاف مثير للاهتمام من خلال تعديل حديث على مشروع القانون، وبالتالي، فإن DPB لا تتعلق فقط بالبيانات الشخصية، ولكن أيضا بالبيانات غير الشخصية، وفقا للجنة المسؤولة عن المشروع، يتعلق الأمر بتوفير حماية أكثر شمولاً للمواطنين، لا سيما في الحالة التي قد تكون فيها حتى البيانات مجهولة المصدر خطيرة بسبب طبيعتها الاستراتيجية (Chavanne, 2022).

بالنسبة لإرشاد معالجة وحماية البيانات ذات الطابع الشخصي وحماية البيانات ذات الطابع الشخصي في الدول العربية، فإن تحليل التشريعات العربية التي عالجت هذه المواضيع ومقارنتها مع بعض التشريعات العالمية، يمكننا من تسليط الضوء على النقاط التي أغفلتها التشريعات العربية بهدف مساعدة الحكومات العربية على معالجتها وتنظيمها من خلال سن وتعديل تشريعاتها الموجودة أو إصدار قرارات أو تنظيمات خاصة تتعلق بحماية البيانات الشخصية، خصوصا مع مشروع الميتافيرس الذي يعد تحديا قانونيا واستراتيجيا واقتصاديا كبيرا يجب مواكبه بإصدار لوائح تكفل حماية مصالح الدولة وخصوصية بيانات مواطنيها (آسيا، 2021).

ضمن هذا السياق تبرز ضرورة الأخذ بعين الاعتبار الخبرات الدولية والإقليمية المتراكمة مع تركيز خاص على «توجهات الاتحاد الأوروبي» في هذا المجال لأجل صياغة الإرشاد الخاص بمعالجة وحماية البيانات ذات الطابع الشخصي والتي تشتمل بشكل رئيسي على:

- الشروط العامة المطلوبة لقانونية معالجة البيانات ذات الطابع الشخصي: تتناول مبادئ متعلقة بنوعية البيانات ذات الطابع الشخصي ومواصفاتها، ومبادئ متعلقة بقانونية معالجة البيانات أي الحالات التي يسمح فيها بمعالجة بيانات ذات طابع شخصي، وتحديد فئات خاصة من المعالجات، بالإضافة إلى الموجبات المفروضة على المسؤول عن المعالجة أو ممثله، وحق الشخص المعني بالاطلاع على خصائص المعالجة المتعلقة به وعلى البيانات المتعلقة به، وطلب تصحيح أو محو أو منع الدخول إلى البيانات المتعلقة به، كذلك حق الشخص المعني بالاعتراض على معالجة البيانات ذات الطابع الشخصي المتعلقة به وذلك لأسباب مشروعة ومرجحة وكذلك لغايات الترويج التجاري، أو الاعتراض على نقل هذه البيانات للغير لغايات الترويج التجاري، ويتناول هذا الموضوع أيضا موجبات المسؤول عن المعالجة لجهة سرية وأمان المعالجات ولجهة استعمال وسائل تقنية وتنظيمية ملائمة من أجل حماية البيانات ذات الطابع الشخصي من التدمير، العرض الغير

مشروع والتعديل والبت أو الوصول الغير المشروع والمعالجة غير المشروعة، وكذا موجبات المسؤول عن المعالجة بالتقدم أمام سلطة الرقابة الرسمية المختصة، للحصول على التصريح والترخيص المسبق منها، وتحديد بيانات التصريح المطلوبة ونشر المعالجات في سجل خاص للمعالجات مفتوح للاطلاع من قبل كل شخص.

- سلطة الرقابة الرسمية المختصة : تتناول إنشاء سلطة رقابة رسمية للسهر على حماية البيانات الشخصية، وتلقي التصاريح حول معالجة البيانات الشخصية وإعطاء التراخيص حول معالجة البيانات الشخصية وإعطاء التراخيص لتنفيذ هذه المعالجات، صلاحيات سلطة الرقابة تشمل جانب التحقيق مثل جمع المعلومات والوصول للبيانات وصلاحياتها التنفيذية لجهة فرض عقوبات إدارية كغرامات أو منع الدخول أو محو البيانات أو وقف المعالجة مؤقتا أو نهائيا واللجوء إلى القضاء كتدابير أكثر فعالية، كما تملك سلطة الرقابة صلاحية تلقي أي طلبات أو شكاوى من الأفراد ومتابعتها بغية ضمان تطبيق عملي فعال للقانون مع ضرورة الالتزام بحفظ السريته.

- المراجعات القضائية، المسؤوليات والعقوبات: تتناول الحق لكل شخص بمراجعة المحاكم المختصة في حال التعرض لأي من حقوقه المتعلقة بمعالجة البيانات ذات الطابع الشخصي وذلك بالإضافة إلى المراجعة الإدارية المتاحة أمام سلطة الرقابة الرسمية المختصة، بالإضافة أيضا إلى الحق في الحصول على تعويض من جراء أي عمل غير مشروع أو خاطئ والحالات التي يعفى فيها المسؤول عن المعالجة كليا أو جزئيا، والتدابير المناسبة لضمان تنفيذ أحكام حماية البيانات الشخصية.

- نقل البيانات ذات الطابع الشخصي إلى دول أجنبية: تتناول شروط نقل البيانات إلى بلد أجنبي والمعايير المفروضة لتقويم مستوى حماية معالجة البيانات الشخصية شرط موافقة الشخص المعني على نقل البيانات الخاصة به والضمانات المفروض أن يقدمها المسؤول عن المعالجة لجهة حماية الحياة الخاصة والحريات والحقوق الأساسية للأشخاص.

- قواعد التصرف: تتناول ضرورة وضع واعتماد قواعد للتصرف تساهم في حسن تطبيق أحكام حماية البيانات ذات الطابع الشخصي، بالإضافة إلى تسوية المعالجات المنفذة والمهلة المحددة لها لكي تصبح متوافقة مع أحكام الارشاد الخاص بها.

خاتمة

لا يمثل ما قدمناه في متن مقالنا هذا سوى جزء مما يثيره مشروع الميتافيرس الضخم، والذي أثرنا من خلاله ضرورة أن يكون المستخدم على دراية كافية بأن بياناته الحيوية ستكون موضع تسويق أكبر عبر هذا المشروع الجديد تبعاً لنوع وحجم البيانات المجمعة عنه، والبحث أكثر في آليات تخزين البيانات الشخصية، وموقعهم ونظام نقل البيانات عبر الحدود، يجب أن تؤخذ هذه الأسئلة العديدة في الاعتبار من قبل المختصين والجهات الفاعلة التي تقوم بتطوير هذه الأكواد الافتراضية من أجل النظر في اللوائح التي ستطبق على الميتافيرس لحماية خصوصية البيانات.

بصرف النظر عن المرور بحركة الثورة التكنولوجية القادمة التي يمثلها مشروع الميتافيرس، يبدو أنه لا توجد حماية كاملة فقط الوقائية تعمل وتقتصر على الاحتياجات الحقيقية للاستخدام، من الضروري للغاية أن يدرك المستخدمون العالم الرقمي الذي يحيط بهم فهذه فجوة كبيرة، في الوقت الحالي نحن نعاني من مشكلة رقمية وعلى المستخدم أن يأخذ وقته الكافي لتعليم نفسه قبل أن يلج هذا الفضاء الجديد.

إن المتداول من القوانين الضامنة لحماية خصوصية البيانات يبرز فجوة كبيرة وتفاوتاً في مواكبة اللوائح القانونية لمشروع الميتافيرس وما يطرحه من تحديات قانونية وحقوقية، ففي حين تبرز اسبقية الاتحاد الأوروبي في هذا المجال تحاول بعض الدول مواكبة هذا الانشغال عبر اثناء ترسانتها القانونية مثل الهند، على أن الدول العربية تبقى متأخرة لافتقادها لميكانزمات واستراتيجية واضحة في هذا الصدد، ولنا أن نقر في الأخير أن البعد الأمني والاستراتيجي لمشروع الميتافيرس يفرض على الدول حماية مصالحها ومصالح مواطنيها عبر الاندماج في كل الورشات المفتوحة لرسم آليات حماية خصوصية بيانات مواطنيها ونقل تجارب الدول الرائدة في هذا المجال فقاطرة التحولات تقودها التكنولوجية وعلى القوانين أن تواكبها تأطيراً وحماية لمصالح الدول والأفراد.

قائمة المراجع

- Abhinov Chandan, D. W. (2021). *dernieres-nouvelles*. Récupéré sur <https://dernieres-nouvelles.com/la-confidentialite-des-donnees-dans-les-contours-du-monde-virtuel-les-complexites-du-metaverse>
- Ball, M. (2022). *The Metaverse and How it Will Revolutionize Everything*. Royaume uni : Norton and company.
- Berendes, p. (2022). *Voyage au centre du METAVERS - Le décrypter, le comprendre et se lancer*. France : Editions Kawa.
- Boilenson, j. (2018). Récupéré sur psycnet : <https://psycnet.apa.org/record/2019-04570-000>

Chavanne, V. (2022). *journal du net*. Récupéré sur <https://www.journaldunet.com/ebusiness/publicite/1506557-l-inde-face-a-la-protection-des-donnees-le-data-protection-bill-enjeux-juridiques-et-geostrategiques>

Faucomprez, P. (2022). *Use your law*. Récupéré sur <https://www.useyourlaw.com/la-reglementation-du-metaverse/>

Legay, a. (2022). <https://www.rtf.be/article/dans-le-metaverse-nos-mouvements-sont-aussi-des-donnees-personnelles-une-menace-importante-pour-notre-vie-privée-10922287>.

(2021). (أسيا, ل. ا). *uneswca*. Récupéré sur https://archive.unescwa.org/sites/www.unescwa.org/files/page_attachments/dir-4-dataprotection.pdf

مستخلص

يبرز الميتافيرس كمشروع أعلنه Mark Zuckerberg لعالم جديد يتجاوز بكثير العالم الذي نعرفه اليوم، عالم يتيح للأفراد القيام بأي شيء تقريبا يمكن تخيله: العمل، والتعلم، واللعب، والشراء، والإنشاء... بمعزل عن العالم المادي، سينغمس الداخل في ثانيا هذا العالم الجديد تماما في عالم رقمي جديد بدون أي حدود، في الوقت نفسه، سيعرض المستخدمون لهذا العالم الجديد بيانات شخصية أكثر من ذي قبل مما يزيد من صعوبة حمايتها أكثر مما هي عليه الآن، فكل ما يفعله المستخدم في هذا العالم الجديد يمكن استغلاله لصالحه أو ضده، كما ستزداد إمكانية تقديم الإشهار بشكل أكثر استهدافا مما هو عليه اليوم بفضل البيانات الحيوية والسلوكية « المعززة »، لذلك فمن المناسب التفكير من الآن في مواجهة هذا العالم الجديد المعلن عنه أين ستبدو اللوائح القانونية الحالية متجاوزة، ومن ثم التفكير دون تأخير في آليات الحماية المستقبلية لخصوصية بيانات المستخدمين في هذا العالم الجديد من خلال تناول ما هو متداول من لوائح واقتراح ما هو ضروري لتعزيز هذه الحماية.

كلمات مفتاحية

الخصوصية، البيانات، الميتافيرس، آليات، الحماية

Résumé

Metaverse, un projet annoncé par Mark Zuckerberg, se présente comme un nouveau monde bien au-delà du monde que nous connaissons aujourd'hui, un monde qui permet aux gens de faire presque tout ce qu'ils peuvent imaginer : travailler, apprendre, jouer, acheter, créer... indépendamment du monde physique. A l'intérieur de ce nouveau monde, le contenu sera complètement immergé dans un nouveau monde numérique sans aucune frontière, en même temps, les usagers exposeront, dans ce nouveau monde, plus de données personnelles qu'auparavant, ce qui rendra encore plus difficile leur protection. Tout ce que fait l'utilisateur dans ce nouveau monde peut être exploité pour ou contre lui, et la possibilité de faire de la publicité augmentera de manière plus ciblée qu'aujourd'hui grâce à des données biométriques et comportementales « enrichies ».

Dès lors, il convient de réfléchir dès maintenant face à ce nouveau monde annoncé où les réglementations apparaîtront inadaptées, puis de réfléchir sans tarder aux futurs mécanismes de protection des données des utilisateurs dans ce nouveau monde en abordant ce qui est en cours et en proposant ce qui est nécessaire pour renforcer cette protection et l'adapter aux exigences nouvelles.

Mots-clés

Vie privée, Données, Métaverse, Mécanismes, Protection

Abstract

Metaverse, a project announced by Mark Zuckerberg, presents itself as a new world far beyond the world we know today, a world that allows people to do almost anything they can imagine: work, learn, play, buy, create... independently of the physical world. Inside this new world, the content will be completely immersed in a new digital world without any borders, at the same time, users will expose, in this new world, more personal data than before, which will make it even more difficult their protection. Everything the user does in this new world can be exploited for or against them, and the possibility of advertising will increase in a more targeted way than today thanks to "enriched" biometric and behavioral data.

Therefore, it is appropriate to reflect now in the face of this announced new world where the regulations will appear unsuitable, then to reflect without delay on the future mechanisms for protecting user data in this new world by addressing what is in progress and by proposing this necessary to strengthen this protection and adapt it to new requirements.

Keywords

Privacy, Data, Metaverse, Mechanisms, protection