الفرصة 36
هل يمكن أن نستخدم تقنيات التشفير المتقدمة لحماية هوياتنا الرقمية؟

حماية الهوية الرقمية الشخصية

يمكن أن يُستخدم تقنيات التشفير المتقدمة (مثل التشفير الكمومي) لحماية الصور الرمزية (الأفاتار) في الواقع الرقمي، بما يضمن إنشاء بيئة موثوقة تعزز الإبداع والتجارة والأمن.

التوجهات العالمية الكبرى
تزايد الثغرات التكنولوجية الأمنية

الاتجاهات السائدة
الأمن السيبراني
الفن والتصميم في العالم الرقمي
الميتافيرس
الواقع الافتراضي

القطاعات المتأثرة
الأمن السيبراني وأمن المعلومات
علم البيانات والذكاء الاصطناعي وتعلم الآلة
التقنيات الغامرة

الواقع الحالي

يشهد العالم الرقمي نمواً متزايداً، وهو ما زاد بالتالي من استخدام الصور الرمزية (الأفاتار) للتنقل بحرية في العالم الرقمي، حيث يترك كل تفاعل لكل صورة رمزية في هذه البيئة الافتراضية سلسلة من نقاط البيانات. وكلما توسع استخدام تقنيات الواقع الرقمي، كلما ازداد عدد الصور الرمزية وزادت نقاط البيانات التي تنتج عنها. وتشير التقديرات إلى أن جلسة واحدة في الواقع الافتراضي تبلغ مدتها 20 دقيقة بإمكانها أن تولد ما يصل إلى مليوني نقطة بيانات حول لغة جسد الفرد، وربما تكشف عن أي اضطرابات في صحته العقلية أو البدنية.[627]

ربط هذه البيانات بالبيانات المالية أو بيانات التواصل أو الاتصال التي يتم جمعها في العوالم الرقمية، يجعل الصور الرمزية هدفاً رئيساً للهجمات الإلكترونية. وكلما زاد استخدام الصور الرمزية، زاد تعرضها لخطر الاحتيال والتزوير، بل وسرقة الهوية الكاملة للصور الرمزية، وهي عملية تُعرف باسم السطو الإلكتروني.[628]

وتشكل الصور الرمزية جزءاً لا يتجزأ من الواقع الرقمي، لا سيما فيما يتعلق بمجال الألعاب الإلكترونية، الذي يضم حالياً حوالي 3 مليارات لاعب حول العالم،[629] وارتفع إيراداته بنسبة 32٪ بين عامي 2019 و 2021، وتشير التقديرات إلى أنها سترتفع بمعدل نمو سنوي مركب يتجاوز 8٪ حتى عام 2026، ما سيؤدي إلى زيادة قيمة هذه الصناعة لتصل إلى 321 مليار دولار.[630]

بالإضافة إلى ذلك، تشكل الصور الرمزية أيضاً جوهر الواقع المعزز والواقع الافتراضي. وقد بلغت قيمة سوق الواقع المعزز والواقع الافتراضي 15 مليار دولار في عام 2020 ومن المتوقع أن تصل إلى 454 مليار دولار بحلول عام 2030 بمعدل نمو سنوي مركب يبلغ 40,7٪.[631] وفي دولة الإمارات على وجه التحديد، من المخطط أن يضيف الواقع المعزز والواقع الافتراضي 4 مليارات دولار إلى اقتصاد الدولة بحلول عام 2030.[632]

يوجد حوالي

3 مليارات

مستخدم للألعاب الإلكترونية حول العالم

الفرصة المستقبلية

الصور الرمزية تمثل الأفراد في العالم الافتراضي.[633] لذلك، ستشكل حمايتها من الضرر (وكذلك حماية الآخرين منها) حاجة ملحة في المستقبل، لا سيما في العالم الرقمي، حيث قد لا يدرك بعض الأفراد أثر الأضرار التي قد يتعرضون لها أو يتسببون فيها في هذا العالم نتيجة لعدم حدوث أذى بدني في الواقع. إضافة إلى ذلك، قد تصبح الصور الرمزية نفسها شخصيات قانونية منفصلة ومستقلة يمكن التحكم بها بواسطة الذكاء الاصطناعي.[634]

في هذا السياق، قد يساعد التشفير الكمومي بشكل كبير في حماية الصور الرمزية، وهوية الأشخاص وبياناتهم، من الهجمات الإلكترونية والانتهاكات التي قد تحدث عن طريق الخطأ. لذلك، فإن تعزيز أمن الصورة الرمزية من شأنه أن يزيد أيضاً من موثوقية البيئة الافتراضية، ومن ثمّ نمو النماذج الاجتماعية والتجارية الجديدة في مساحات الواقع الرقمي ونجاحها. كما يمكن استخدام هذه التقنية من التشفير للتحقق من الاتفاقيات وعمليات الشراء والمحتوى الإبداعي، الأمر الذي يقلل من التكاليف ويحد من خطر التزييف أو التزوير. إضافة إلى ذلك، قد تعزز الصور الرمزية المحمية بواسطة التشفير الكمومي ثقة الأفراد والمجتمع في الواقع الرقمي، خصوصاً إذا تم تعديل التشريعات، وربما وضع لوائح جديدة تتعلق بالصور الرمزية تشمل حالات الاحتيال وسرقة الهوية والتشهير وغيرها من الجرائم.[635]

الفوائد

رفع مستوى الأمان في التعاملات وتخفيض تكلفتها وتحسين التفاعل الاجتماعي، ما يسهم في نمو الواقع الرقمي واستقراره.

المخاطر

اختراق التشفير الكمومي بشكلٍ غير ملحوظ، ما يسمح للنسخ المزورة من الصور الرمزية باختراق بيانات حساسة لأغراض إجرامية أو تجسسية، بالإضافة إلى بطء وتيرة تطور النظم القانونية، وبالتالي عدم مواكبتها للنهج الكمومي في مجال التشفير، مما يجعل بدوره تنفيذها أمراً متعذراً.

إن جلسة واحدة في
الواقع الافتراضي تبلغ مدتها 20 دقيقة
بإمكانها أن تولد ما يصل إلى

2 مليون

نقطة بيانات حول لغة جسد الفرد