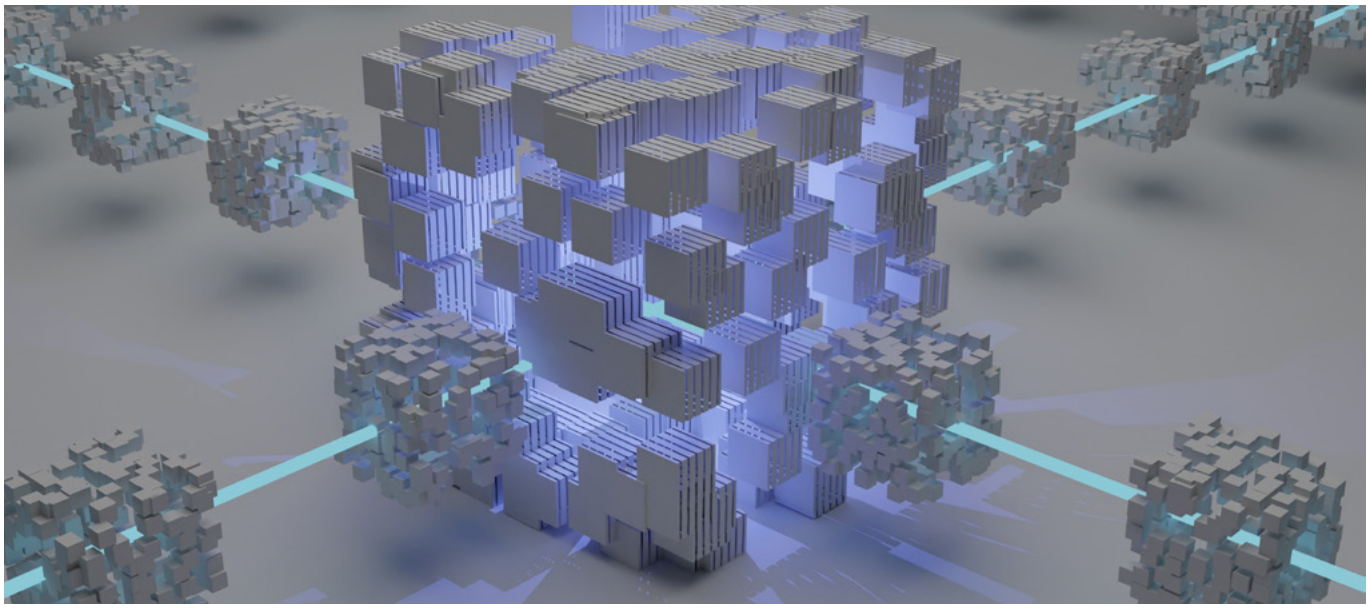
الفرصة 38
ماذا لو حولنا بياناتنا الشخصية والحساسة إلى رموز مشفرة؟

تحويل البيانات الحساسة إلى رموز مشفرة

سيتمكن الأفراد من تحويل بياناتهم الشخصية الحساسة لرموز مشفرة، ومن ثمّ الحفاظ على دقتها ونزاهتها، والتحكم في تحديد المصرّح لهم بالوصول إليها، وربما الاستفادة منها تجارياً.



التوجهات العالمية الكبرى
تزايد الثغرات التكنولوجية الأمنية

الاتجاهات السائدة
الذكاء الاصطناعي
حماية البيانات والخصوصية
نظام الرموز المشفرة

القطاعات المتأثرة
المواد والتقنية الحيوية
تقنية المعلومات والاتصالات
أمن المعلومات والأمن السيبراني
علم البيانات والذكاء الاصطناعي وتعلّم الآلة
الصحة والرعاية الصحية
التأمين وإعادة التأمين
الخدمات الحكومية

الواقع الحالي

في ظل توقع ارتفاع المعدل السنوي للجرائم الإلكترونية إلى 15٪ في الفترة من 2022 إلى 2025، من المتوقع أيضاً أن تبلغ التكاليف المرتبطة بهذه الجرائم 10.5 تريليون دولار في جميع أنحاء العالم بحلول العام 2025، ما يشكل زيادة بنسبة 300٪ تقريباً مقارنة مع مستويات العام 2015.[646] وتشير التقديرات إلى أن الفوائد الاقتصادية المرتبطة بضمان أمن الهوية الرقمية ستتراوح بين 3٪ و 13٪ من الناتج المحلي الإجمالي بحلول العام 2030.[647]

ورغم أن 137 دولة من أصل 194 دولة على مستوى العالم (ما يعادل 71٪ من الدول تقريباً) قد أقرت تشريعات لحماية الخصوصية والبيانات الشخصية، إلا أن تبني هذه القوانين حقق مستويات متدنية في أفريقيا بواقع 61٪ وفي آسيا 57٪.[648]

في الوقت نفسه، بلغ المتوسط العالمي لإجمالي تكلفة اختراق البيانات في عام 2022 حوالي 4.35 مليون دولار. وفي مجال الرعاية الصحية، بلغ متوسط إجمالي تكلفة خرق البيانات بنحو 42٪ منذ عام 2020 ليصل إلى نحو 10 مليون دولار[649]. وتعد سرقة أو اختراق البيانات الشخصية أكثر عمليات خرق البيانات شيوعاً ويستغرق تحديدها وقتاً طويلاً يصل إلى 327 يوماً.[650] وبما أن نصف حالات اختراق البيانات تقع في السحابة، فقد بلغ متوسط تكلفة اختراق البيانات لدى المؤسسات التي تعتمد على نموذج هجين للسحابة نحو 3.80 مليون دولار، وهو أقل من التكلفة التي تتكبدها المؤسسات المعتمدة على نموذج السحابة التقليدي العام (5 مليون دولار) أو الخاص (4.2 مليون دولار).[651]

غير أن الجرائم الإلكترونية لا تؤدي إلى تكبد تكلفة اقتصادية فحسب، بل تؤثر أيضاً على صحة الأفراد. إذ كشفت نتائج استبيان أنّ 70٪ من ضحايا الاحتيال بدت عليهم علامات القلق أو التوتر أو الاستياء أو الإحباط عندما تم تحذيرهم من احتمال وقوع عملية احتيال.[652] وتشير التقديرات إلى أن تكلفة الرعاية النفسية لضحية الاحتيال تصل إلى 3000 أو أكثر، بينما تصل التكلفة المادية نحو 700 دولار تقريباً.[653]

ويتوقع أن يصل حجم السوق المستهدف لحماية البيانات إلى 100 مليار دولار، مع العلم أنه لا يتم حالياً تلبية سوى 30٪ إلى 35٪ من الطلب في هذا السوق.[654]

أقرت

٪71

من دول العالم تشريعات لحماية الخصوصية والبيانات الشخصية

الفرصة المستقبلية

سوف تحقق الرموز المشفرة نقلة نوعية في الأسواق المالية[655] وتزوّد الأفراد بفرصة مشاركة بياناتهم الحساسة عن طريق تحويلها إلى قيمة أو منفعة نقدية، مع إمكانية الاحتفاظ ببعض العناصر الأساسية من البيانات لاستخدامها لاحقاً، كما في أغراض تدريب النماذج التنبؤية للعلاجات الجديدة لمرض السرطان - على سبيل المثال.

وبهذه الطريقة، يتم استخدام البيانات وعناصرها الحساسة الأصلية (التي تضمن عزو البيانات إلى أصحابها من الأفراد أو العائلات) وتخزينها كمثال خارج قاعدة البيانات المستخدمة في تدريب النماذج التنبؤية لعلاجات السرطان الحديثة. وتوفر تقنيات الرموز المشفرة مزايا عديدة مقارنة بالتشفير العام، إذ لا يمكن فك تشفير تلك الرموز المميزة أو الرجوع عنها.

ومن البديهي أن يزيد إقبال الأفراد على مشاركة بياناتهم الحساسة عند التأكد التام من عدم إمكانية تتبع تلك البيانات أو حتى الكشف عنها عن طريق الخطأ. وكلما زادت مشاركة الأفراد لبياناتهم، زادت مساهمتهم في الابتكارات الطبية والعلمية وتحسين عملية صناعة السياسات المجتمعية.

الفوائد

ستؤدي أنظمة مشاركة البيانات الأكثر شفافية إلى خلق المزيد من الثقة، لا سيما عند مشاركة البيانات في المجالات الحساسة مثل الصحة والتعليم، إضافة إلى تحقيق المزيد من المكاسب سواء للأعمال أو أفراد المجتمع من خلال تعزيز القيمة المقدمة للأفراد الذين يقومون بإنشاء البيانات ومشاركتها.

المخاطر

اختراق الرموز المشفرة على نطاق واسع وبطرق متطورة، والاعتماد على استقرار الشبكة والتقنيات المرتبطة بها، واتساع الفجوات الاقتصادية الناجمة عن الهوامش في قيمة الرموز المشفرة الشخصية.

من المتوقع أن تبلغ التكاليف المرتبطة **بالجرائم الإلكترونية**

10.5 تريليون دولار

في جميع أنحاء العالم بحلول العام 2025،

ما يشكل زيادة بنسبة

٪300

مقارنة مع مستويات العام 2015