حماية البيانات الشخصية عبر تقنية البلوك تشين

Protecting personal data via block chain technology

إعداد

الدكتور/ ياسر محمد النيداني

مدرس القانون المدني

معهد العجمي العالي للعلوم الإدارية

البريد الإلكتروني : yasermoh014@gmail.com

ملخص البحث

تتناول هذه الدراسة موضوع حماية البيانات الشخصية عبر تقنية البلوك تشين ، وذلك من خلال البحث في اللائحة الأوربية لحماية البيانات الشخصية(GDPR) باعتبارها اللائحة الأكثر صعوبة وشهرة في العالم في مجال حماية البيانات الشخصية ، مع الاسترشاد بالأحكام القضائية الصادرة عن محكمة العدل الأوربية ومحكمة التمييز الفرنسية وكذلك الاسترشاد بآراء فرق العمل الأوربية المعنية بموضوع حماية البيانات الشخصية في البلوك تشين، وآراء اللجنة الوطنية لتكنولوجيا المعلومات والحريات الفرنسية(CNIL).

تطرقت هذه الدراسة لتقنية البلوك تشين بطريقة مبسطة ؛ وذلك حتى يستطيع غير المتخصص فهم خصوصيات هذه التقنية ، كما تمت دراسة البيانات الشخصية وصورها بشكل عام ، ليلحقها بعد ذلك دراسة للبيانات الشخصية في البلوك تشين وحقوق صاحب البيانات على هذه البيانات والمتمثلة في الحق في الوصول، الحق في التصحيح، الحق في المحو، ، الحق في إمكانية نقل البيانات، الحق في الاعتراض والحق في تقييد المعالجة.

خلصت هذه الدراسة إلى أن تقنية البلوك تشين تبدو غير متوافقة مع قوانين حماية البيانات الشخصية ، حيث تقدم اللائحة العامة لحماية البيانات الحقوق على البيانات الشخصية ، والتي تتعارض في جوهرها مع نظام البلوك تشين غير القابل للتغيير.

كما عرضت الدراسة الحلول المقترحة في محاولة للتوفيق بين البلوك تشين ومتطلبات اللائحة العامة للبيانات بخصوص حماية حقوق المستخدم على بياناته الشخصية.

الكلمات المفتاحية : البلوك تشين ، البيانات الشخصية ، اللائحة العامة لحماية البيانات (GDPR) ، حقوق مستخدم البلوك تشين.

Research Summary

This study addresses the issue of protecting personal data via blockchain technology, through research into the European Personal Data Protection Regulation (GDPR), as it is the most difficult and famous regulation in the world in the field of personal data protection, while being guided by judicial rulings issued by the European Court of Justice and the French Court of Cassation. As well as being guided by the opinions of the European working groups concerned with the issue of personal data protection in blockchain, and the opinions of the French National Committee for Information Technology and Liberties (CNIL).

This study touched on blockchain technology in a simplified manner. This is so that a non-specialist can understand the peculiarities of this technology. Personal data and their images were studied in general, followed by a study of personal data in the blockchain and the rights of the data subject over this data, which are the right to access, the right to correction, the right to erasure, the right. In data portability, the right to object and the right to restrict processing.

This study concluded that blockchain technology appears to be incompatible with personal data protection laws, as the General Data Protection Regulation introduces rights over personal data, which are inherently inconsistent with an immutable blockchain system.

The study presented proposed solutions in an attempt to reconcile blockchain with the requirements of the General Data Regulation regarding protecting the user's rights over his personal data.

Keywords: Blockchain, personal data, General Data Protection Regulation (GDPR), blockchain user rights.

١١ - حماية البيانات الشخصية عبر تقنية البلوك تشين

مقدمة

على الصعيد العالمي، ارتفع عدد الأشخاص حول العالم الذين يستخدمون الإنترنت إلى ما يزيد على خمسة مليارات شخص.

أصبح المستخدمون مهتمين بشكل متزايد بالأنشطة عبر الإنترنت ، ومشاركة المحتوى الذي يرغبون فيه. يشارك العديد من المستخدمين بياناتهم الشخصية عبر الإنترنت وهم غير مدركين، أو يعرفون القليل جدًا عن خصوصيتهم والمخاطر المحتملة المرتبطة بها.

من الصعب جدًا فهم التعريف القانوني والفني للبيانات الشخصية ، حيث إن هناك الكثير من الغموض حول تعريف البيانات الشخصية ، وبالتالي يبدو الأمر وكأنه متاهة ؛ نظرًا لصعوبة فهم الأمر، يميل العديد من المستخدمين إلى فعل ما يريدون ، ومشاركة الكثير من المحتوى عبر الإنترنت.

كما ارتفعت المخاوف المتعلقة بالخصوصية في السنوات القليلة الماضية بسبب حدوث العديد من فضائح البيانات(مثل فضيحة كامبريدج أناليتيكا) ، والتي سلطت الضوء على مخاطر تراكم البيانات الشخصية بين جهات فاعلة لا تملك عليها سيطرة تذكر.

أصبحت الخصوصية على الإنترنت مصدر قلق متزايد هذه الأيام للأشخاص من جميع الأعمار ، وأجبرت المستخدمين على إعادة التفكير في علاقاتهم بوسائل التواصل الاجتماعي والتطبيقات ، وأمن معلوماتهم الشخصية.

نظرًا لتطور تقنيات الكمبيوتر والاهتمام بسوق "البيانات" وزيادة المخاوف بشأن الخصوصية فقد أصدر البرلمان الأوروبي ومجلس الاتحاد الأوروبي بتاريخ ٢٥ ابريل ٢٠١٦ اللائحة العامة لحماية البيانات (GDPR) رقم ٦٧٩ / ٢٠١٦ والتي دخلت حيز التنفيذ في ٢٥ مايو ٢٠١٨.

تهدف هذه اللائحة لتكييف الأنظمة مع الواقع الرقمي الجديد ، وبالتالي السماح بالتنسيق الوطني بهدف بناء نظام "السوق الرقمية الموحدة" ، والتي سيكون هدفها من ناحية حماية الأشخاص الطبيعيين فيما يتعلق بمعالجة البيانات الشخصية ، وحرية حركة البيانات ، وتعزيز اقتصادها ، ومن ناحية أخرى مساءلة الجهات الفاعلة خلال معالجة البيانات، وتعزيز العقوبات بشكل كبير.

وقد وصفت مفوضية الاتحاد الأوروبي اللائحة العامة لحماية البيانات بأنها خطوة أساسية لتعزيز الحقوق الأساسية للمواطنين في العصر الرقمي ، توفر أدوات للتحكم في البيانات الشخصية للشخص ، وتهدف إلى حماية الحقوق ، والحريات الأساسية للأشخاص الطبيعيين، وبشكل أكثر تحديدًا الحق في حماية البيانات الشخصية.

١١ - حماية البيانات الشخصية عبر تقنية البلوك تشين

تتمثل الأهداف الأساسية للائحة العامة لحماية البيانات (GDPR) في إعادة السيطرة للمواطنين والمقيمين على بياناتهم الشخصية ، وتبسيط البيئة التنظيمية للأعمال التجارية الدولية من خلال توحيد اللوائح داخل الاتحاد الأوروبي.

كما أن هذه اللائحة منحت حقوقًا مطلقة لأصحاب البيانات ، حيث تمنح المستخدمين أنواعًا مختلفة من الحقوق على بياناتهم : الحق في الحصول على المعلومات، الحق في الوصول، الحق في التصحيح، الحق في المحو، الحق في تقييد المعالجة، الحق في إمكانية نقل البيانات، الحق في الاعتراض، والحقوق المتعلقة باتخاذ القرار الآلي.

من ناحية أخرى يعد أمن البيانات عنصرًا أساسيًا في المجتمعات والشركات والمنظمات ، ويحتاج مستهلكو تكنولوجيا المعلومات (الإنترنت، والحوسبة، والتخزين، وما إلى ذلك) إلى مستوى عالٍ من الأمان لضمان الإدارة السليمة للبيانات الرقمية.

في الحقيقة يعد الجمع الهائل للبيانات الشخصية تهديدًا جديدًا للخصوصية ؛ ذلك أننا نعهد بشكل متزايد بالبيانات الشخصية للشركات والتطبيقات مقابل الوصول المجاني إلى الشبكات الاجتماعية ، أو خدمات المراسلة ، أو غيرها من الخدمات.

يثق المستخدمون في الأنظمة المركزية ، ويعرفون أنفسهم على المنصات الرقمية حيث يرسلون ويستقبلون البيانات، ويخزنون المعلومات.

من المؤكد أن مركزية البيانات يمكن أن توحد جهود أمن البيانات في نظام قوي، ولكن هذا الحل المركزي يطرح العديد من التحديات: حيث يمثل الطرف الثالث الموثوق به نقطة ضعف للاختراق يتم من خلاله نقل البيانات الحساسة ؛ ذلك أن تركيز البيانات في نظام واحد يوفر فرصة للمتسللين، حيث يتيح لهم الوصول إلى كمية كبيرة من البيانات في وقت واحد. كما أنه غالباً ما تتم إدارة الأنظمة المركزية من قبل كيان واحد ، مما يعني عدم وجود آلية لمنع أي شخص من إفساد النظام.

كذلك فإن مركزية البيانات ، والتي يتم تخزينها على خوادم يمكن أن تكون عرضة للهجمات السيبرانية ، والوصول غير المصرح به.

توفر تقنية البلوك تشين (block chain) حلاً لا مركزيًا يمكنه القضاء على نقاط الفشل الرئيسية في الأنظمة المركزية ، كما أن هذه التقنية تمثل حقبة جديدة في طريقة إنشاء الثقة بين فردين.

تقنية البلوك تشين تم اختراعها في عام ٢٠٠٨ من قبل رجل ، أو امرأة ، أو مجموعة من الأشخاص تحت اسم ساتوشي ناكاموتو .لا أحد يعرف من وراء هذا الاسم.

البلوك تشين عبارة عن قاعدة بيانات لا مركزية خالية من الوسطاء تجعل من الممكن أتمتة المعاملة والمصادقة عليها وختمها الزمني من خلال عُقد الشبكة، مع ضمان ثباتها ، وسرية البيانات من خلال التشفير غير المتماثل.

١١ – حماية البيانات الشخصية عبر تقنية البلوك تشين

فالبلوك تشين نظام لامركزي بالكامل، حيث يتم إنشاء الثقة من خلال مشاركة البيانات، والتحقق من صحتها بين عُقد الشبكة، باستخدام الأساليب القديمة المعروفة مثل خوارزميات التشفير غير المتماثل باستخدام المفتاحين العام والخاص، ونظير إلى نظير، والأسماء المستعارة و العناوين الرقمية للعُقد.

معظم المعلومات الموجودة على البلوك تشين العامة مرئية لجميع المشاركين الذين يستضيفون البلوك تشين ، نظرًا لعدم قابلية تغيير السجلات[١]، وموثوقية المعلومات المبنية على الإجماع ، وشفافية المعاملات التي توفرها تقنية البلوك تشين ، فقد تم دمج هذه التكنولوجيا في الصناعات الحساسة والنشطة مثل المدن الذكية.

أصبحت هذه التقنية الجديدة ، التي اشتهرت بفضل البيتكوين، سريعة الانتشار في كل مكان لدرجة أنه يصعب في بعض الأحيان تذكر كيف كانت تبدو الأشياء قبل وصولها.

هذه التكنولوجيا تجتذب اليوم المزيد والمزيد من المشغلين الاقتصاديين : الأعمال المصرفية، والتمويل، وإدارة حقوق الملكية الفكرية، والأحوال المدنية، والصحة..

[١] – كما سنرى لاحقا تعد سلاسل الكتل بمثابة دفاتر للإلحاق فقط ولا يمكن حذف البيانات منها بسهولة بمجرد إضافتها.

وينظر إليها اللاعبون في العديد من القطاعات باعتبارها نموذجًا تنظيميًا يعدهم بإمكانية تتبع وشفافية وكفاءة أفضل لعملياتهم.

غالبًا ما يساء فهم التقنيات الرقمية الجديدة من قبل عامة الناس "بينما ينبغي لنا جميعًا أن نكون متنورين ومندمجين في أرض الخوارزميات ، كما أننا جميعا محكوم علينا بالتكيف باستمرار مع هذه التقنيات الجديدة ؛ حتى لا نتعرض للتقادم المخطط له.

كثيرًا ما يُتهم العديد من اللاعبين في عالم التكنولوجيا بعدم الاهتمام بالقدر الكافي بشأن احترام البيانات الشخصية للمستخدمين.

إن تكنولوجيا البلوك تشين التي نشأت من العملات المشفرة ، لها مستقبل واعد، إلا إن علاقتها بالقانون تبدو غامضة ؛ لأنها تميل إلى تحرير نفسها من القواعد القانونية الكلاسيكية.

أهمية الدراسة : تظهر الأهمية العلمية لموضوع هذا البحث في أنه يقودنا إلى محاولة إدراك وفهم الاستجابات القانونية الإيجابية ، أو السلبية لتكنولوجيا البلوك تشين، وفي المقام الأول من الأهمية ، ومن المحفز أكثر أن ندرس مثل هذه الاستجابة ؛ نظراً للفارق الزمني الذي يمكن العثور عليه بين التكنولوجيا وإطارها القانوني المحتمل.

اشكالية الدراسة: تظهر المشكلة الرئيسة لموضوع هذا البحث في أن استخدام تقنية البلوك تشين غالبا ما يكون مصحوبا بالبيانات الشخصية للمستخدم ، والتي قد تكون مهددة بالاعتداء عليها بأي صورة من الصور، وهذا يستدعى النظر في قدرة القانون الوضعي اليوم على فهم استخدامات وعواقب تكنولوجيا البلوك تشين في طبيعتها الأدبية- حيث إنها تطبيق للصيغ الرياضية ومفاهيم الكمبيوتر- ومعرفة مدى الحماية القانونية الممنوحة للبيانات الشخصية للمستخدم المتوافقة مع تقنية البلوك تشين بحيث لا تشكل عائقًا أمام التطور التكنولوجي لهذه التقنية.

فرضيات الدراسة : يثير موضوع هذا البحث بعض التساؤلات التي تتطلب إجابة عليها وهي على النحو التالي

١-هل يتوافق البلوك تشين مع اللائحة الأوربية العامة لحماية البيانات(GDPR) ؟

٢-من المسؤول فعليًا في تقنية البلوك تشين عن حماية البيانات الشخصية للمستخدم في هذه الشبكة اللامركزية ؟

منهج الدراسة : سوف أعتمد في تناول هذا البحث على المنهج الاستنباطي، إذ سأقوم باستنباط بعض الأحكام التي وردت في اللائحة الأوربية العامة لحماية البيانات (GDPR) التي تُعنى بحماية البيانات الشخصية، وكذلك ما ورد عن الفقه القانوني والأحكام القضائية بشأن حماية البيانات الشخصية عبر تقنية البلوك تشين ؛ وذلك من

أجل الوصول لنتيجة منطقية بخصوص مدى التوافق بين قواعد حماية البيانات الشخصية وتقنية البلوك تشين.

كما أنني سأستخدم المنهج الوصفي التحليلي، حيث سأقوم بتحليل كامل مفصل ومبسط لتكنولوجيا تقنية البلوك تشين ، على أن نتبع ذلك بتحليل مفهوم البيانات الشخصية لمستخدم البلوك تشين وحقوقه على هذه البيانات.

نطاق الدراسة : سوف نقتصر نطاق الدراسة على حماية البيانات الشخصية عبر تقنية البلوك تشين في دول الاتحاد الأوربي باعتباره النطاق المكاني لتطبيق اللائحة الأوربية العامة لحماية البيانات(GDPR) والتي تعد أصعب قانون للخصوصية والأمن في العالم ، كما أنها الأكثر شهرة عالميا بخصوص حماية البيانات الشخصية ، والتي حذت العديد من الدول حذوها لتنظيم حماية وتداول البيانات الشخصية ومنها: البرازيل واليابان وولاية كاليفورنيا بالولايات المتحدة الأمريكية.

خطة البحث :

مقدمة

المبحث الأول: ماهية البلوك تشين.

المبحث الثاني: البيانات الشخصية في البلوك تشين.

المبحث الثالث: حماية حقوق صاحب البيانات الشخصية في البلوك تشين.

المبحث الأول

ماهية البلوك تشين

تعد تقنية البلوك تشين من أهم وأكبر ابتكارات القرن الحادي والعشرين نظرا لتأثيرها على مختلف القطاعات بدءا من المالية إلى التصنيع والتعليم[١].

تقنية البلوك تشين هي قاعدة بيانات معاملات موزعة، يمكن مقارنتها بدفتر المحاسبة اللامركزي والمشترك، الذي يقوم بتخزين ونقل القيمة ، أو البيانات عبر الإنترنت، بشفافية وأمان وبشكل مستقل لأنه بدون هيئة مراقبة مركزية.[٢] تدار بواسطة مستخدميها بلا وسيط ، غير قابلة للتعديل ، أو الإزالة ، تتولى إدارة قائمة متزايدة من الكتل التي تحتوى كلاُ منها على عدد من البيانات والمعلومات[٣].

تمت دراسة الأنظمة الموزعة في مجال البحث منذ فترة طويلة قبل وصول البلوك تشين(block chain). على سبيل المثال، تم اقتراح فكرة تسلسل الكتل مع وظيفة تجزئة التشفير من أجل ثبات البيانات من قبل رالف ميركل في أطروحته للدكتوراه، في

---

[١] – رحاب فايز أحمد سيد ، تقنية البلوك تشين وتوثيق الانتاج الفكري العربي ، مجلة المكتبات والمعلومات الرقمية ، س ٤٠، عدد ٢، ابريل ٢٠٢٠ ص ١٦

[2] - Houiqua Ismail: Utilisation de Blockchain pour la sécurisation des données ERPs, diplôme de master académique Département d'informatique, Faculté des Sciences Exactes, des Sciences de la Nature et de la Vie, Algérie,2021/2022 p.5.

[٣] – أشرف جاد ، البلوك تشين والإثبات الرقمي في مجال حق المؤلف، المجلة الدولية للفقه والقضاء والتشريع ، العدد ١ ، ٢٠٢٠ ص ٣٥.

عام ١٩٧٨، وقد أظهر ميركل في هذا العمل أنه يمكن ربط المعلومات بكفاءة وتنظيم البيانات في بنية شجرة.

في نفس العام، اقترح ديفيد شوم إنشاء نظام موثوق يعتمد على شبكة من الأقران ، وتشتمل اللبنات الأساسية لهذا النظام على "خزائن" آمنة ماديًا، وأساسيات التشفير الموجودة (وظائف التشفير المتماثلة وغير المتماثلة والتجزئة).

بحلول نهاية الثمانينيات أظهر Dwork وLynch وStockmeyer القدرة على حل الإجماع في مجموعة واسعة من الأنظمة "المتزامنة جزئيًا في أنظمة أخرى للسماح للنظام الموزع بالاتفاق على نتيجة ، أو رسالة[١].

في وقت مبكر من عام ١٩٩١ تم وصف البنية الكامنة وراء تقنية البلوك تشين عندما قدم الباحثان ستيوارت هابر ودبليو سكوت ستورنيتا حلاً حاسوبيًا عمليا لختم الوثائق الرقمية بالوقت ، مما يسمح بوضع طابع زمني على المستندات الرقمية وبالتالي عدم تقادمها ، أو تغييرها ، أو تبديلها أبدًا ، وقد استخدم نظامهم بلوك تشين آمنًا للتشفير لتخزين المستندات المختومة بالوقت[٢].

[1] -Mirko Koscina:Security and Optimization of Blockchains and Associated Algorithms,these, École doctorale Sciences Mathématiques de Paris Centre, Université Paris sciences et lettres 2021 p.16

[2] - Ibid - Houiqua Ismail,op.cit.p.7

استخدم النظام سلسلة من الكتل المشفرة لتخزين المستندات المختومة بالوقت. ثم، في عام ١٩٩٢، أضافوا إلى التصميم بناء شجرة ميركل، مما جعله أكثر كفاءة من خلال تمكين جمع العديد من المستندات في كتلة واحدة[١].

لاحقًا، في عام ١٩٩٩، اقترح كاسترو وليسكوف خوارزمية جديدة فعالة لتكرار البيانات قادرة على مقاومة الأخطاء البيزنطية في بيئة غير متزامنة.

في عام ٢٠٠٤، أطلق عالم الكمبيوتر وناشط التشفير **هال فيني** نظامًا يسمى RPoW ("إثبات العمل القابل لإعادة الاستخدام")[٢] يعمل النظام من خلال تلقي رمز إثبات عمل غير قابل للتداول وغير قابل للاستبدال استنادًا إلى نظام Hashcash[٣]، والذي بدوره أنشأ رمزًا مميزًا بتوقيع RSA[٤] والذي يمكن بعد ذلك نقله من شخص لآخر[٥].

---

[1]- Mirko Koscina op.cit.p.16

[٢] - إثبات العمل (PoW) هو شكل من أشكال إثبات التشفير حيث يثبت أحد الأطراف (المثبت) للآخرين (المتحققين) أنه تم إنفاق قدر معين من الجهد الحسابي المحدد ويمكن للمحققين بعد ذلك تأكيد هذه النفقات بأقل جهد من جانبهم.

[٣] –Hashcash هو نظام إثبات العمل يستخدم للحد من البريد الإلكتروني العشوائي وهجمات رفض الخدمة.

[٤] – تعتمد خوارزمية RSA على تقنية تشفير المفتاح العام لنقل البيانات بشكل موثوق ، حيث تتمتع بصلابة غير عادية ، حيث إن اقتحام المفاتيح بواسطة المعترضات أمر صعب للغاية.

[5] - Houiqua Ismail,op.cit.p.7

في نهاية عام ٢٠٠٨، قدمت ورقة بيضاء نظام دفع إلكتروني لامركزي من نظير إلى نظير، **يسمى بيتكوين.** تم توزيع الورقة البيضاء عبر قائمة بريد إلكتروني متعلقة بالتشفير من قبل فرد ، أو مجموعة من الأفراد مجهولين باستخدام الاسم المستعار ساتوشي ناكاموتو[١].

تعتمد شبكة البيتكوين على خوارزمية إثبات العمل HashCash، ولكن بدلاً من استخدام وظيفة حوسبة موثوقة مثل RPoW، يتم توفير حماية الإنفاق المزدوج من خلال بروتوكول نظير إلى نظير لامركزي لتتبع المعاملات والتحقق منها[٢].

في الثالث من يناير عام ٢٠٠٩، ظهرت للنور عملة البيتكوين بعد أن تم إلحاق أول كتلة تم تعدينها بالسلسلة.

قام ساتوشي ناكاموتو بتعدين الكتلة الأولى، وحصل على ٥٠ بيتكوين. كان أول مستلم للبيتكوين هو هال فيني، الذي تلقى عشرة عملات بيتكوين من ساتوشي ناكاموتو في أول معاملة بيتكوين في العالم في ١٢ يناير ٢٠٠٩.

[1]- Houiqua Ismail,op.cit.p.7 - Audrey Side, Benjamin Mollet -Vieville, et AugustinCordin, Master 2 Droit de la propriété intellectuelle appliquée Université Paris Est Créteil 2017-2018,p.15

[2] - Houiqua Ismail,op.cit.p.7

١١ – حماية البيانات الشخصية عبر تقنية البلوك تشين

في عام ٢٠١٣، كشف المبرمج والمؤسس المشارك لمجلة البيتكوين، **فيتاليك بوتيرين**، لمجتمع البيتكوين عن الحاجة إلى لغة برمجة نصية لبناء تطبيقات تعمل فوق شبكة البلوك تشين.

بعد ذلك، بدأ بمشروع إيثريوم لبناء نظام حوسبة موزع جديد يعتمد على البلوك تشين مع وظيفة البرمجة النصية لإنشاء تطبيقات موزعة، تسمى العقود الذكية.

تكتسب تقنية البلوك تشين اليوم الكثير من الاهتمام السائد ويتم استخدامها بالفعل في تطبيقات مختلفة، ولا تقتصر على العملات المشفرة[١].

إذا كنا نسلم بأن تقنية البلوك تشين ليست هى الأولى التي تقوم بتخزين وحفظ وتبادل البيانات بين المستخدمين في شكل خوارزميات، وتبنى تقنية التشفير غير المتماثل إلا أنها تتميز عن غيرها من التدابير التي تقوم بتلك الوظائف بما تنفرد به من قدرة على الموائمة بين كل هذه الأدوار وبين وظائفها المستحدثة.

سوف استعرض في هذا المبحث تعريف البلوك تشين في المطلب الأول ، والبلوك تشين ، وقواعد البيانات التقليدية في المطلب الثاني.

[1] - Mirko Kosciva op.cit.p.12.

المطلب الأول

تعريف البلوك تشين

سوف نتعرض في هذا المطلب لتوضيح ما هو البلوك تشين ، هيكله ، أنواعه ، وكيفية اتمام المعاملة على البلوك تشين وتكلفتها.

أولا : ما هي سلسة الكتل (البلوك تشين)

الخطوة الأساسية الأولى هي محاولة فهم ما تغطيه هذه التكنولوجيا. يكمن أصل البلوك تشين في البحث عن طريقة لتخزين البيانات وتبادلها بشكل آمن[١].

في الشبكة اللامركزية، لا توجد سلطة رقابية تصادق على أصل ، أو سلامة الرسائل المرسلة. إذًا، كيف يمكننا ضمان موثوقية نقل المعلومات عبر مكونات الكمبيوتر؟.

في الدراسة التي نشرها ثلاثة متخصصين في التشفير عام ١٩٨٢، كانت الفكرة هي إيجاد حل لموثوقية عمليات الإرسال وإدارة فشل واحد ، أو أكثر من مكونات نظام الكمبيوتر، على سبيل المثال نقل المعلومات المتناقضة[٢].

[1] - Mustapha Mekki, Les mystères de la blockchain Recueil Dalloz 2017 p.2160 n° 3

[2] - Claire Leveneur, Les Smart Contracts,Étude De Droit Des Contrats À L'Aune De La Blockchain.Thèse,Doctoral School of Private Law,Université Paris-Panthéon-Assas.2022 p.58 n° 64

١١ - حماية البيانات الشخصية عبر تقنية البلوك تشين

الاستعارة التي يستخدمها علماء التشفير هي تلك الخاصة بالجنرالات البيزنطيين[١]: الإمبراطور غائب عشية هجوم كبير، ومن الضروري أن يهاجم جميع الجنرالات في وقت واحد. كيف يمكن التأكد من وقت الهجوم من قبل كل من الجنرالات؟

حيث يكون هناك مجموعة جنرالات يحاصرون مدينة معادية، لكي يكون الهجوم فعالاً فإنه يتطلب تنسيقًا مثاليًا بين مختلف الجنرالات. مع ذلك، يمكن أن يكون هناك خونة بينهم يتسببوا في فشل مهمتهم. للقيام بذلك التنسيق، من المناسب استخدام وسيلة اتصال غير قابلة للتزوير وغير قابلة للتغيير والتي لا يمكن اعتراض بياناتها. هذه هي الحاجة التي تهدف تقنية البلوك تشين إلى معالجتها[٢].

لفهم استخدامات البلوك تشيين لنتخيل مواطنًا أجنبيًا يرغب في تجديد تصريح إقامته في مصر ، سيتعين عليه الحصول على سلسلة كاملة من الوثائق من مؤسسات مختلفة ومن ثم إبلاغها إلى الوكيل الإداري المختص.

في هذه العملية الكلاسيكية ليس هناك ما يضمن عدم تزوير المستندات التي تمر عبر يدي مقدم الطلب. كما أنه ليس من غير المألوف أن يشير الوكيل لمقدم الطلب إلى أن إحدى المستندات مفقودة.

---

[1] - Mustapha Mekki,op.cit. n° 3
[2] - Claire Leveneur , op cit p.58 n° 64

بفضل تقنية البلوك تشين ، التي من المفترض أن توفر الأمان المطلق، لن تمر المستندات عبر مقدم الطلب ويمكن تقديم الوثيقة المفقودة بسرعة أكبر، دون الحاجة إلى تحديد موعد جديد، وبتكلفة أقل. يتيح لنا هذا المثال الحصول على فكرة بديهية أولى عن افتراضيات البلوك تشين.

البلوك تشين عبارة عن "آلية برمجية لا مركزية تسمح بتتبع وتسجيل الأصول والمعاملات دون وجود سلطة ثقة مركزية مثل البنك، وتنشئ شبكات بلوك تشين إثباتاً للملكية باستخدام التوقيعات الرقمية الفريدة، التي تعتمد على مفاتيح التشفير العامة المعروفة للجميع على الشبكة والمفاتيح الخاصة المعروفة فقط للمالك، بحيث تدل الخوارزميات المعقدة إلى توافق الآراء بين المستخدمين، مما يضمن عدم إمكانية العبث ببيانات المعاملات بعد التحقق، الأمر الذي من شأنه تقليل المخاطر"[١].

ثانيا : هيكل البلوك تشين

يتكون البلوك تشين من ثلاثة أجزاء رئيسية وهى الشبكة والكتلة والتجزئة.

[١] – قميتى عفاف ، واقع وافاق استخدام تقنية البلوك تشين في اقتصاديات المنطقة العربية ، مجلة أبحاث اقتصادية معاصرة ، المجلد ٦، العدد ١ ، ٢٠٢٣ ص ١٤.

١- **الشبكة** : تتكون الشبكة من "العقد الكاملة". فهي كجهاز كمبيوتر يقوم بتشغيل خوارزمية لتأمين الشبكة. تحتوي كل عقدة على سجل كامل لجميع المعاملات التي تم تسجيلها في ذلك البلوك تشين [١].

٢- **الكتلة** : قائمة المعاملات المسجلة في دفتر الأستاذ (السجل) خلال فترة زمنية معينة. يختلف الحجم والفترة والحدث المحفز للكتل لكل البلوك تشين.

ليس الهدف الأساسي لجميع سلاسل الكتل هو تسجيل وضمان سجل لحركة عملاتها المشفرة. لكن جميع سلاسل الكتل تسجل حركة عملتها المشفرة ، أو رمزها المميز. فكر في المعاملة على أنها مجرد تسجيل للبيانات ، يتيح لك تعيين قيمة لها (كما هو الحال في المعاملة المالية) ، وتفسير ما تعنيه هذه البيانات [٢].

فالكتلة عبارة عن الوعاء الذي يحمل البيانات التي يتم حفظها على البلوك تشين، وهي

وحدة بناء السلسلة، حيث تضم السلسلة الواحدة عدداً من الكتل ، والتي تضم فئة من المعاملات المتماثلة التي يتم إجراؤها داخل السلسلة، وترتبط فيما بينها بتوقيع رقمي موحد يضمن سلامة المعاملة بقيدها في لحظة حدوثها، ويتم حفظ هذه المعاملات

[1] - Houiqua Ismail,op.cit.p.10
[2] - Houiqua Ismail,op.cit.p.9

داخل الكتلة، وتصبح نهائية لا يمكن التراجع عنها ، أو تغييرها ، ويتم تسجيل المعاملة لدى جميع الأشخاص الذين لديهم نسخة من السجل[١].

٣- **التجزئة** : تعتبر التجزئة لبنة أساسية في تقنية البلوك تشين ، حيث يتم استخدامها لإثبات سلامة الكتل ، وإنشاء رابط بين الكتل المتتالية التي بنيت عليها السلسلة. فهي الغراء[٢] الذي يربط ويجمع كل صفحة من صفحات دفتر الأستاذ (السلسلة).

تعد التجزئة نوع من التشفير في البلوك تشين ؛ ذلك أنها عبارة عن سلسلة مشفرة من الحروف والأرقام التي تكون فريدة بشكل دائم لكل كتلة فردية في التسلسل المتسلسل؛ يُطلق عليها أحيانًا أيضًا "البصمة الرقمية"[٣].

يتم إنشاء التجزئة في البلوك تشين من البيانات الموجودة في الكتلة السابقة، وهي بصمة لهذه البيانات التي تقفل الكتل بالترتيب وبمرور الوقت.

تعتبر وظائف التجزئة المشفرة أساسية لتشغيل العملات المشفرة ، ومن خلالها تتمتع البلوك تشين بمستوى عالٍ من الأمان وسلامة بياناتها. فهي تنفذ تسلسلات من

[١] - سعاد صالح أحمد أبوبكر، توجهات وتحديات تقنية البلوك تشين في حماية البيانات وضمان الخصوصية، المجلة الأفريقية للعلوم البحتة والتطبيقية المتقدمة (AJAPAS)، المجلد ٢، العدد ٣، يوليو-سبتمبر ٢٠٢٣، ص٣٥

[٢] - التجزئة هي السحر الذي يلصق الكتل معًا ويسمح لها بخلق الثقة الرياضية Houiqua Ismail,op.cit.p.9

[3] - Houiqua Ismail,op.cit.p.10.

العمليات لتأمين نقل المعلومات بين عدة أنظمة، وتسمى نتائجها "التوقيعات" ، أو "بصمات الأصابع". تتميز وظائف التجزئة أيضًا بحتميتها، فطالما ظل المدخل المستخدم كما هو، فإن خوارزمية التجزئة تنتج نفس البصمة بشكل منهجي[١].

تستخدم التجزئة لتسلسل كتل متتالية حيث يتم إنشاء سلسلة الكتل من خلال الإشارة إلى الكتلة السابقة ، كما يتم استخدامها للإشارة إلى الموقع الذي يتم تخزين البيانات فيه(يشير مؤشر التجزئة إلى العنوان حيث يتم تخزين بيانات الكتلة السابقة) ؛ لذلك يمكن استخدام مؤشر التجزئة للتحقق مما إذا كان قد تم التلاعب بالبيانات أم لا[٢].

بالإضافة إلى ذلك، يمكن للمستخدمين التحقق علنًا من تجزئة البيانات المخزنة لإثبات عدم تعديل البيانات المخزنة.

إذا حاول أحد الخصوم تعديل البيانات في أي كتلة تابعة للسلسلة، فيجب عليه تغيير مؤشرات التجزئة الخاصة بالكتل السابقة لإخفاء التلاعب؛ لذلك، يحتاج الخصم إلى تغيير جميع المؤشرات في جميع الكتل حتى الوصول إلى الكتلة الأولى (كتلة التكوين) والتي يتم إنشاؤها بمجرد إنشاء النظام ، وهذا يعني أن الخصم يحتاج إلى استثمار الكثير من الموارد لينجح في هجومه.

[1] - Houiqua Ismail,op.cit.p.10
[2] - Mirko Koscina,op.cit.p20

وأخيرًا، تجبر مؤشرات التجزئة الخصم على إعادة بناء السلسلة لينجح في هجومه ، وإلا سيتم كشف العبث الذى قام به[١].

هكذا تكون سلسلة الكتل مصممة ومشفرة على نحو يضمن المحافظة على البيانات المخزنة بها، ويحول دون أي تعديل عليها، مع إضفاء الطابع الزمني لها، مع توثيق كل معاملة بتوقيع إلكتروني متمثل في المفتاحين الخاص والعام، وتُعرف هذه العملية، أي عملية حفظ الكتلة على هذا النحو ببروتوكول البلوك تشين[٢].

ثالثا : أنواع البلوك تشين.

لقد تطورت تقنية البلوك تشين بسرعة في السنوات القليلة الماضية. في الوقت الحالي، من الممكن العثور على أنواع مختلفة من هياكل شبكة البلوك تشين. ولدت هذه البنى الجديدة بسبب حالات الاستخدام والأنظمة البيئية المختلفة حيث يمكن تنفيذ الخدمات القائمة على البلوك تشين[٣].

غالبًا ما يُشار إلى البلوك تشين (سلاسل الكتل) في اللغة الإنجليزية باسم "DLT" (تقنية دفتر الأستاذ الموزع) وهو المصطلح الذي يتم العثور عليه بشكل متكرر في الكتابات الفرنسية[٤].

---

[1] - Mirko Koscina,op.cit.p20

[٢] – سعاد صالح أحمد أبوبكر، المرجع السابق ص ٣٧

[3] - Mirko Koscina,op.cit.p.21.

[4] - Claire Leveneur ,op.cit.p.70 n° 86

ومع ذلك، فإن هذا الاستخدام مضلل، حيث إن البلوك تشين والدفاتر الموزعة ليسا مترادفين ؛ لأن البلوك تشين هو في الواقع مجرد حالة خاصة من دفاتر الأستاذ الموزعة DLT.

يشير مصطلح البلوك تشين ، كما يُستخدم المصطلح عمومًا، إلى فئة من دفاتر الأستاذ الموزعة باستخدام تقنية هيكلة بيانات البلوك تشين ؛ لذا فإن جميع سلاسل الكتل عبارة عن دفاتر موزعة ، ولكن ليست كل دفاتر الأستاذ الموزعة عبارة عن سلاسل كتل؛ وذلك لأنها لا تستخدم بشكل منهجي هيكلة البلوك تشين ، أو آلية إجماع الأغلبية، والتي تشكل اختلافين رئيسيين عن سلاسل الكتل الأكثر تقليدية[١].

تعتمد تقنية البلوك تشين على تنفيذ بنية لا مركزية، وهكذا، بدلًا من وجود هيئة مركزية تمتلك وحدها المستندات التي توزع نسخًا منها على العملاء، يمتلك كل كمبيوتر ملفات مجموعة[٢].

تحقق هذه اللامركزية ثلاث فوائد رئيسية: تعزيز أمن النظام ، وإزالة أي نشاط وسيط ، وضمان صحة المعاملات[٣].

---

[1] - Ibid.p. 71 n° 86

[2] - Thibaut Labbe,Le droit face aux technologies disruptives : le cas de la blockchain,These,Universite De Strasbourg ,École Doctorale ,2021.p.18. n° 13

[3] - Ibid.18. n° 14

يمكن تطبيق هذه الاهتمامات الرئيسية الثلاثة في ثلاثة أنواع من البلوك تشين وهى البلوك تشين العام ، البلوك تشين الخاص ، البلوك تشين الهجيني (كونسورتيوم).

إذا كنا نتحدث في أغلب الأحيان عن "البلوك تشين" بطريقة غير متمايزة ، فذلك يعني تحديد النوع الأكثر انتشارًا من البلوك تشين وقبل كل شيء بما يتوافق مع البلوك تشين الأولي، وهو البلوك تشين العام.

ولكن تم تطوير أنواع أخرى من البلوك تشين لتلبية الاحتياجات الأخرى. تمت إزالة خصائص معينة من الانفتاح واللامركزية ؛ لتقييد الوصول إلى السجل ، وربما تزيد من تأمين هذه الأنواع الجديدة من البلوك تشين: هذه هي البلوك تشين الخاصة والبلوك تشين الهجينية (كونسورتيوم).

١ : البلوك تشين العام.

في التصميم الكلاسيكي والأصلي لبروتوكولات البلوك تشين [١] يجب أن تكون الشبكة الموزعة – التي تكون برمجياتها مفتوحة المصدر – متاحة للعامة.

[١] –إن سلاسل الكتل العامة هي سلاسل الكتل الحقيقية الوحيدة وفقًا للأصوليين ، وتشمل هذه المجموعات سلاسل العملات المشفرة (البيتكوين، والإيثيريوم، وما إلى ذلك) والتي يقال إن هناك ١٦٠٠ منها– عام ٢٠١٩– وهي مفتوحة للجميع للقراءة والكتابة ومفتوحة المصدر، بحيث يمكن لأي شخص استخدامها أو إنشاء برنامج للوصول إليها.
Thibault Douville,Blockchain et protection des données à caractère personnel, AJ contrat 2019 p.316 n° 4.

وبالتالي فإن بروتوكولات البلوك تشين مفتوحة ومتاحة للجميع، سواء للقراءة ، أو الكتابة دون قيود، ودون خضوع أي العمليات لقبول طرف ثالث.

تتميز تقنية البلوك تشين العامة بأنها تتحقق في شكل سجل عام يمكن لأي مستخدم في العالم قراءته ، وإرسال المعلومات إليه ، وتنفيذ المعاملات التي سيتم تسجيلها في السجل.

هذا هو الحال، على سبيل المثال، بالنسبة للبيتكوين، وهو عبارة عن بلوك تشين عام ، يمكن للجميع الوصول إليه[١].

تتميز تقنية البلوك تشين العامة بأنها تُمكن كل مشارك في الشبكة من بدء المعاملات عن طريق إرسال البيانات الموقعة بواسطة مفتاحه الخاص ، والتشاور مع أي معاملة يتم تنفيذها على الشبكة، ويتم الحفاظ على سرية هوية مؤلفي المعاملات من خلال الشاشة التي يتم تشكيلها باستخدام المفتاح العام و المفتاح الخاص.

ثانيًا، ليس هناك حاجة إلى إذن ، أو تصريح لكتابة البيانات ، أو قراءتها ؛ ولهذا السبب تسمى هذه البروتوكولات العامة "بلا إذن".

ثالثًا، غالبًا ما تستخدم بروتوكولات البلوك تشين بروتوكول الإجماع الذى يهدف إلى منع الانشاء المتزامن للكتل ، وتجنب انشاء سجلات موازية.

[1] - Audrey Side et al. op.cit.p.2

كما أنه لا أحد يتحكم في الشبكة، إنما تخضع عملية التحقق من صحة الكتلة المفتوحة للجميع ، والتي تسمى التعدين ، ويمكن لأي مستخدم (شريطة أن يكون لديه القدرة الحاسوبية اللازمة) المشاركة بحرية في هذه العملية والموافقة على المعاملات التي يتم تنفيذها في البلوك تشين [١].

تساعد عملية التحقق على الحماية من مخاطر الهجمات الضارة ، ويؤدى تضاعف عدد العُقد إلى زيادة التحقق من الكتل ، مما يجعل البلوك تشين أكثر موثوقية ضد التلاعب الضار بالبيانات[٢].

تعد سلاسل الكتل المفتوحة (بدون إذن) قليلة العدد (البيتكوين والإيثريوم)، رغم أن المحتوى الابتكاري لها هو الأكثر أهمية ، ولكن إمكاناتها التكنولوجية لم يتم تخصيصها بشكل كافٍ من قبل القطاعات الاقتصادية المختلفة[٣].

هناك بروتوكولات بلوك تشين تم تطويرها بشكل مختلف من أجل الحد من الوصول إلى البيانات المتبادلة ، وتعيين عدد قليل فقط من المشاركين للتحقق من صحة المعاملات: وهذه إما بلوك تشين خاصة ، أو شبه خاصة تسمى بلوك تشين "اتحاد"[١].

---

[1] - Audrey Side et al. op.cit.p.2.

[2]- Cédric Strub , Contribution De La Blockchain Au Management Des Donnees De Sante , Memoire De Diplome D'État De Docteur En Pharmacie,Université de Strasbourg Faculté de Pharmacie,2020.p.22

[3] - Rapport de la mission médiatique conjointe ,Informations sur la blockchain et ses usages (1) : L'enjeu de la souveraineté de décembre 2018 p.3

٢: البلوك تشين الخاص.

تعتبر سلاسل الكتل الخاصة أقل لا مركزية ، ولكنها تعمل بسرعة أكبر[٢]. في البنية المرخصة يمكننا إنشاء تكوينات مختلفة وفقًا للاحتياجات المحددة. في هذه الحالة، يمكننا تكوين شبكة البلوك تشين مع التحكم الكامل في جميع العقد من قبل مؤسسة واحدة ، و يُطلق على هذا التكوين اسم البلوك تشين الخاص[٣].

البلوك تشين الخاص منصة مغلقة ومحاطة بالقيود، إذ إنها تخضع لوسيط يُحكم سيطرته وقبضته عليها، ويستطيع التحكم في ضوابط استخدام الشبكة في الوقت الذي يراه ، وهذه المنصة عادةً ما تستخدمها المؤسسات المصرفية[٤].

يجب تسجيل كل مستخدم للشبكة في سلطة مركزية قبل الانضمام إليها. بالإضافة إلى ذلك، في هذا التكوين، يتم التحكم في العقد من قبل منظمة واحدة ، ومن ثم فإن صيانة وتشغيل شبكة البلوك تشين تعتمد على كيان واحد.

---

[1] - Claire Leveneur, op.cit.p.71.

[2] - Rapport de la mission médiatique conjointe ,Informations sur la blockchain et ses usages.2018 op.cit. p.3

[3] - Houiqua Ismail,op.cit.p.23

[٤] – جهاد محمود عبد المبدي ، مدى حجية تقنية البلوك تشين في الإثبات المدني"دراسة تحليلية" المجلة الدولية للفقه و القضاء والتشريع المجلد ٤، العدد١ فبراير ٢٠٢٣ ص ٧٦

قد تكون أذونات القراءة عامة ، أو مقيدة إلى حد تعسفي ، وبالتالي قد لا تكون القراءة العامة ضرورية في كثير من الحالات ، على الرغم من أنه في حالات أخرى، تكون المراجعة العامة مرغوبة[١].

يتم حجز الوصول إلى الشبكة ، واستخدامها لجهات فاعلة معينة ، ويتم التحقق من صحة المعاملات بواسطة عدد محدود من العُقد[٢]. فهي تجمع بين العديد من الجهات الفاعلة– في كثير من الأحيان كيانات قانونية مثل الشركات – وبعدد محدود ؛ لتسهيل إدارة مصالحها المتبادلة[٣].

جميع المشاركين في الشبكة معروفون ، ويثقون ببعضهم البعض مسبقًا ؛ لذلك يلزم الحصول على إذن للوصول إليها، ولهذا السبب تسمى سلاسل الكتل هذه "البلوك تشينات المرخصة"[٤].

---

[1] - Houiqua Ismail,op.cit.p.22

[٢] – تتحكم المؤسسة في الشبكة، وتتحكم في الأشخاص المسموح لهم بالمشاركة، وتشغيل بروتوكول الإجماع. Houiqua Ismail,op.cit.p.12

[٣] – يمكن أن تكون طبيعة المصدر المفتوح في البلوك تشين العام مزعجة للبعض لأنها قد تسمح، في حالة إمكانية الوصول إلى النظام، "بكسر" الكود دون الحاجة إلى الاستفادة من السجل اللامركزي.

Thibault Verblest,Blockchain : une révolution juridique ?Revu Lamy Droit des Afferes N°129 SEPTEMBRE 2017.p.51

[4] - Claire Leveneur, op.cit.p.72

١١ - حماية البيانات الشخصية عبر تقنية البلوك تشين

على عكس البلوك تشين العامة، تحتاج البلوك تشين الخاصة فقط إلى ثلاثة مشاركين لتشغيلها، في حين تحتاج البلوك تشين العامة إلى عدة آلاف من المشاركين لتنمو.

يمكن مقارنة البلوك تشين العام بالإنترنت، في حين يمكن مقارنة البلوك تشين الخاص بالإنترانت، لديهما أوجه تشابه قوية، ولكن أساليب التشغيل الخاصة بهما مختلفة بشكل كبير[١].

يبتعد هذا النظام عن التصميم النقي للبلوك تشين. في هذا النوع من البلوك تشين، يمكن تحديد ثلاث خصائص:

أولاً، يقوم كيان (أو مجموعة كيانات) بإعداد البروتوكول، والتحكم في الشبكة ، وتعيين القائمين بالتعدين.

بعد ذلك، يتم اختيار المشاركين مسبقًا ؛ ليتمكنوا من الوصول إلى الشبكة ، و يجب عليهم تلبية المتطلبات المحددة عند الإدخال ، أو الحصول على ترخيص من مسؤول البلوك تشين.

أخيرًا، من الممكن أن يوفر النظام استخدام بروتوكول الإجماع، ولكن يمكن أيضًا تحديد حالة السجل وفقًا لرأي المسؤول أو مجموعة فرعية من المشاركين[٢].

يعد المثال الأكثر شهرة لسلاسل الكتل المسموح بها هو Hyperledger Fabric[١].

[1] - Cédric Strub op.cit.p.23-24.
[2] - Claire Leveneur, op.cit.p.72 n° 89

٣ : البلوك تشين المغلق "الكونسورتيوم"(الاتحاد)

في سلاسل كتل "الكونسورتيوم" تمتزج خصائص الفئتين المذكورتين ، حيث يعد دفتر الأستاذ هذا تطبيقًا مختلطًا بين دفتر الأستاذ غير المصرح به ودفتر الأستاذ الخاص[٢].

يعد اتحاد البلوك تشين مثاليًا للشركات عندما يحتاج جميع المشاركين إلى الحصول على تصريح ، وتحمل مسؤولية مشتركة عن البلوك تشين [٣].

ينتج هذا البلوك تشين عن تجميع العديد من المنظمات المستقلة ، أو حتى المتنافسة، التي تستخدم تقنية البلوك تشين ؛ لأرشفة المعاملات الآمنة في سجل لامركزي، أو تبادل الأعمال المعتمدة، دون الحاجة إلى إشراك طرف ثالث موثوق به[٤].

وبالتالي، تتحكم عدة كيانات في الشبكة ، وتحدد قواعد الإدارة ، وحقوق الوصول إلى الشبكة، والتي يمكن أن تختلف اعتمادًا على الجهات الفاعلة ، والاستخدامات (سيكون لدى بعض الجهات الفاعلة فقط إمكانية الوصول إلى البيانات المتعلقة بها، وما إلى ذلك).

علاوة على ذلك، يتم تحديد المتغيرات بواسطة بروتوكول الشبكة ، وتتعلق بدرجة المركزية التي يسعى إليها مسئولو البلوك تشين.

---

[1] - Mirko Koscina,op.cit.p.22
[2] - Ibid.
[3] - Houiqua Ismail,op.cit.p.12.
[4] - Cédric Strub ,op.cit.p.22.

أخيرًا، من الممكن تشفير الكتل ؛ حتى يتمكن الجميع من معرفة وجودها ، ورؤية سلسلة الكتل بأكملها، مع منح حق الوصول إلى محتوى الكتل للبعض فقط من خلال الضغط على مفتاح التشفير المطلوب[١].

رابعا: اتمام المعاملة على البلوك تشين

يتضمن تشغيل البلوك تشين معظم الأدوات التكنولوجية الموصوفة: شبكة نظير إلى نظير، وقاعدة بيانات موزعة، وأدوات التشفير ؛ لضمان أمان الشبكة ، وسلامة التبادلات بين الأعضاء ، والإجماع وآلية الحوافز ؛ لمكافأة عُقد الشبكة.

سنوضح فيما يلى كيف تتم المراحل المختلفة من بدء المعاملة حتى إدراجها بشكل لا يمحى في البلوك تشين ، كما سنتعرض لتكلفتها وذلك على النحو التالي:

أ-بدء المعاملة على البلوك تشين.

بداية يجب علينا أن نبين أن المعاملة هي مجرد تسجيل لبيانات ، وذلك يتيح لنا تعيين قيمة لها (كما هو الحال مع البيانات المالية).

يجب على المستخدم الجديد للبلوك تشين تنزيل البرنامج من موقع الويب المخصص.

غالبا ما يعتمد البلوك تشين على برمجيات مفتوحة المصدر/مجانية (أي متاحة مجانًا من قبل مؤلفيها) ، ولكن في ظل ظروف معينة[١].

[1] - Claire Leveneur op.cit.p.72

يتم تعيين كل من المشاركين في مثل هذا البروتوكول على أنه "عقدة" ، وتتكون الشبكة التي تستخدم بروتوكول البلوك تشين من العديد من العقد المرتبطة ببعضها البعض بواسطة شبكة شبكية، يتم نسخ البيانات المستخدمة وحفظها بواسطة كل منها[٢].

سيقوم مستخدم البلوك تشين بإنشاء معرف ، مما يسمح له بامتلاك كلا المفتاحين العام والخاص[٣] ، المفتاح العام له ؛ ليتم بثه بشكل عام على الشبكة، والمفتاح الخاص ؛ ليتم الاحتفاظ به بشكل آمن[٤].

يستخدم البلوك تشين التشفير غير المتماثل[١] لتنفيذ المعاملة التي تحتوى على المعلومات المقصود تخزينها في قاعدة بيانات البلوك تشين ، وتحديد المشاركين ، وتوقيع المعاملات[٢]:

---

[1] - Cédric Strub ,op.cit.p.14.

[2] - Cédric Strub ,op.cit.p.14 n° 9

[3] - Thibaut Labbe. op.cit.p.22.

[٤] - مسألة السرية أمر ضروري لأنه بدون السرية لا توجد ثقة، وبدون ثقة لا يوجد مستخدمون. في هذه الحالة، تسمح تقنية البلوك تشين للمستخدم بالبقاء مجهول الهوية عن طريق مجموعة من مفاتيح التشفير – غير المتماثل– المخصصة له والتي تجعل من الممكن التعرف على المستخدم. وبشكل ملموس، سيسمح المفتاح الخاص الأول للمستخدم بتنفيذ عملية ما ، أما المفتاح الثاني العام فسيسمح للشبكة بالتحقق من قدرتها بالفعل على تنفيذ العملية.

Sébastien Drillon,La révolution Blockchain,La redéfinition des tiers de confiance,RTD Com. 2016 p.893 n° 11.

يشار إلى التشفير بأنه غير متماثل ؛ نظرا لأن المفتاح العام والمفتاح الخاص لا يلعبان نفس الدور، ويمكن توضيح هذا النظام من خلال إيداع شيء ما في خزنة بمفتاحين. سيتمكن حاملو المفتاح العام من وضع الأشياء في الخزنة دون أن يتمكنوا من إزالتها، ولن يتمكن سوى حامل المفتاح الخاص من إزالة العناصر من الخزنة[٣].

يتم توقيع المعاملة باستخدام مفتاح خاص من المشارك إلى واحد أو أكثر من المشاركين المجهولين المعروفين فقط بالمفاتيح العامة ، حيث يقوم بإرسال المعاملة مشفرة ، وموقعة باستخدام مفتاحه الخاص[٤] في شكل رسالة ، ليتم التحقق منها بواسطة عُقد الشبكة. وبالتالي يتم إنشاء توقيع رقمي فريد من خلال الجمع بين المفتاح الخاص ورسالة المعاملة.

---

[١] – تقليديًا، لإرسال رسالة مشفرة، تم استخدام التشفير لتشفير الرسائل وفك تشفيرها، بحيث يكون لدى كل مستخدم هذا الرمز. وتكمن المشكلة في انتشار كود التشفير، مما يضعف الحماية الممنوحة. ثم تم تطوير التشفير ليصبح غير متماثل بفضل العمل المنشور في عامي ١٩٧٦ و١٩٧٨ . وهذا التقدم يجعل من الممكن الآن إنشاء اتصال سري بين شخصين دون إثبات مسبق للسرية. Claire Leveneur, op.cit.p.59

[2] - Thibaut Labbe. op.cit.p.16.- Kahina Khacef,Trade-Off Between Security And Scalability In Blockvhain Systems, Thesis, Doctoral School of Computer Science, Telecommunications and Electronics. Sorbonne University, 2022.p.54.

[3] - Audrey SIDE et al. op.cit n° 11

[4] - Cédric Strub ,op.cit.p.19

النتيجة هي أن المعاملة التي تم البدء بها هي اسم مستعار (وليست مجهولة المصدر) حيث لا يوجد بيانات تحدد هوية المصدر مباشرة ، باستثناء عنوانه العام الذي يتكون من تسلسل أبجدي رقمي[١].

عندما يتم تنفيذ معاملة ما داخل البلوك تشين، يتم التحقق من شروط إتمامها من قبل جميع الخوادم المتصلة (وتسمى أيضًا العُقد)، وفي حالة النجاح في التحقق من العملية يتم ختم الأخيرة بالوقت ، ثم تتم إضافتها خلال فترة زمنية. "كتلة"، يتم وضعها في سلسلة الآخرين، المشتركة بين الخوادم المختلفة المشاركة في البلوك تشين، وبالتالي دمج هذه المعاملة بطريقة زمنية ، وغير قابلة للتزوير في سجل ثابت غير قابل للتغيير[٢].

تنشأ هذه الطبيعة المقاومة للتلاعب من أن كل معاملة يتم تنفيذها تحت غطاء بروتوكول البلوك تشين يتم توقيعها من قبل مؤلفها ولم يتم تزويرها من قبل طرف ثالث[٣] ، كما أن التحقق منها يتم من قبل جميع المشاركين في الشبكة، ثم يتم ختمها زمنيًا ، ليتم مشاركتها بين هؤلاء المشاركين أنفسهم داخل قاعدة البيانات المشتركة

[1] - Claire Leveneur, op.cit.p.62.
[2] - Thibaut Labbe. op.cit.p.14.
[3] - Claire Leveneur, op.cit.p.63 n° 72

بينهم. سيتم تنفيذ هذه المعاملة في كتلة، والتي ستأتي بعد المعاملات الأخرى المسجلة بالفعل (ومن هنا جاء اسم البلوك تشين"block chain")[١].

يتكون البلوك تشين من عدد من الكتل المتصلة تسلسليًا، وكل كتلة في السلسلة لها أصلها، أي الكتلة السابقة عليها ، في حين أن الكتلة الأولى على الإطلاق في السلسلة تسمى كتلة التكوين[٢].

تحتوى كل كتلة على مجموعة من المعاملات التي يقوم بها أعضاء (أي عمال المناجم) في البلوك تشين [٣] ، ولإضافة كتلة جديدة إلى البلوك تشين ، يجب على جميع أعضاء السلسلة التوصل إلى اتفاق، ويشار إلى هذا باسم الإجماع[٤].

[1] - Thibault Verblest op.cit.p15 n° 9

[2] - Hajar Moudoud,Intégration de la Blockchain à l'Internet des Objets.,these, Universite De Technologie De Troyes en Science Pour L'Ingenieur.2022.p.16

[٣] – الكتلة هي قائمة المعاملات المسجلة في دفتر الأستاذ (السجل) خلال فترة زمنية معينة. يختلف الحجم والفترة والحدث المحفز للكتل لكل البلوك تشين.

Houiqua Ismail,op.cit.p.9

[٤] - الإجماع هو اتفاقية للتحقق من صحة البلوك تشين، والتي ترتبط بترتيب وتوقيت الكتلة. هدفها هو تحقيق اتساق العقد المشاركة في البلوك تشين. تقبل جميع العقد الصادقة نفس ترتيب المعاملات طالما تم تأكيدها في طرق عرض البلوك تشين المحلية الخاصة بها. يتم تحديث البلوك تشين باستمرار مع استلام كتل جديدة. Kahina Khacef op.cit.p.52

يوفر الإجماع اليقين بأن العُقدة الصادقة فقط هي التي يمكنها تحديث السلسلة الرئيسية. ستعتمد عملية اختيار العُقدة الصادقة التي لها الحق في إضافة كتلة جديدة على نوع تطبيق البلوك تشين[١].

يمكن أن تختلف خوارزمية الإجماع اعتمادًا على بنية البلوك تشين ، إلا أن الهدف الرئيسي دائمًا هو فرض قواعد أمان منصة البلوك تشين ومنطق الأعمال.

يجب أن تتفق جميع العُقد على قيمة واحدة باتباع بروتوكول الإجماع. بعد ذلك نعتبر النظام متسامحًا مع الأخطاء إذا توصلت معظم العقد إلى اتفاق حتى عندما تكون أقلية من اللاعبين ضارة وقد تنحرف عن البروتوكول بشكل تعسفي[٢].

في معظم سلاسل الكتل، يتم التوصل إلى الإجماع عندما يعتقد أكثر من ٥٠٪ من العُقد أن المعاملة معتمدة وتم التحقق منها، وبالتالي يمكن إضافتها – داخل كتلة – إلى البلوك تشين[٣].

لفهم تقنية البلوك تشين سوف نستعير المثال الذى استخدمه **تيبو لابي**[٤]: يوجد عدد محدود من الطلاب في غرفة مقسمة إلى نفس العدد من المكاتب بقدر عدد الطلاب، وجميعهم يشاهدون سلة من التفاح.

---

[1] - Mirko Koscina ,op.cit.p15.

[٢] - يسمى هذا بالتسامح مع الخطأ البيزنطي Mirko Koscina,op.cit.p.27

[3] - Claire Leveneur, op.cit.p.61

[4] - Thibaut Labbe. op.cit.p.12-13.

١١ - حماية البيانات الشخصية عبر تقنية البلوك تشين

يمكن لكل طالب رؤية السلة، ولكن ليس بشكل كامل أبدًا (فقط مجموعة رؤى الطلاب الحاضرين ستجعل من الممكن الحصول على عدد كافٍ) لكنهم لا يستطيعون التفاعل مباشرة مع بعضهم البعض ، ويبقون معزولين بشكل فردي ، وبالتالي، ليس لدى كل منهم سوى جزء من المعلومات النهائية للعثور عليها ، ويجب أن ينجحوا في تحديد العدد الدقيق للتفاح.

مع ذلك، يمكنهم التواصل مع بعضهم البعض، ولكن سمك الأقسام يعني أن المعلومات تستغرق دائمًا قدرًا معينًا من الوقت للوصول إليها ، وهم مقسمون إلى عدد كبير من المكاتب ، ولا يمكنهم الاجتماع ، ناهيك عن وجود شخص موثوق به ينقل معلومات موثوقة فيما بينهم.

من بين هؤلاء الطلاب بعض "الأغبياء" الذين لا يريدون الكشف عن عدد التفاح ؛ لذلك فإنهم سوف يحذفون المعلومات، أو يقدمون معلومات غير صحيحة، أو حتى يظلوا صامتين.

التحدي الذي يواجههم هو تحديد العدد الدقيق للتفاح في السلة ، وبالتالي فإن صعوبة هذا الموقف تكمن في كيفية تمكن الطلاب ، في ظل وجود العديد من المعلومات المحتملة سواء كانت موثوقة أم لا، من أن يقرروا معًا العدد الدقيق للتفاح في السلة.

هنا تصبح الرياضيات مهمة؛ لأنه في الواقع، تتيح الخوارزمية تحقيق هذا الهدف (تحديد عدد التفاح)، مع مراعاة الأخطاء المحتملة (عدم رغبة الطلاب في الكشف عن عدد التفاح)

تم تصميم هذه الخوارزمية من قبل عالم الكمبيوتر ليزلي لامبورت، وتجد تطبيقات كثيرة في قطاع تكنولوجيا المعلومات.

هذه هي روح تقنية البلوك تشين: استخدام الإجماع بين الجهات الفاعلة الموثوقة ، وغيرهم ممن قد يجدون أنفسهم فاشلين في تمكين عملية صنع القرار.

كل طالب (حتى أولئك الذين لا يريدون الكشف عن عدد التفاح) من بين العدد المحدود الأولي سيقترح حلاً (يوجد عدد س من التفاح) ، وسيتم تقديم كل حل من الحلول لموافقة جميع الطلاب، الذين سيقبلون ، ككل، أو لا يقبلون الحل الذي يقترحه كل منهم.

سيتم حساب كل حل من الحلول ، وإدخاله في سجل يمكن لجميع الطلاب الوصول إليه ، ومن خلال التصويت سيحدد هذا المجتمع عدد التفاح بأغلبية الأصوات. إذا تم تسجيل جميع الإجابات التي تم عدها من قبل الطلاب، فسيتم تطبيق فقط تلك التي تعتبر موثوقة ، وبالتالي سيتم تحديد عدد التفاح من قبل المجتمع ، وسيتم اعتباره موثوقًا ؛ لأنه حصل على دعم الأغلبية.

١١ - حماية البيانات الشخصية عبر تقنية البلوك تشين

يفرض الإجماع مجموعة من الضوابط الرئيسية ، وهي اقتراح كتل جديدة في البلوك تشين ، وبروتوكول القراءة للتحقق الآمن من البلوك تشين ، وأخيرًا، اتساق سجلات البيانات المضمنة في كل إصدار محلي من البلوك تشين التي تحتفظ بها كل عُقدة.

سوف يلتزم كل نظير بالكتل الجديدة عند القيام بإجراءات الإجماع اللامركزي الناجحة في البلوك تشين [١].

بمجرد التوصل إلى إجماع بين جميع الأعضاء، يتم التحقق من صحة الكتلة الجديدة ثم إضافتها إلى السلسلة، وستشير كل كتلة جديدة إلى الكتلة السابقة لها مباشرة (أي الكتلة الأصلية).

تضمن تقنية البلوك تشين أنه بمجرد إضافة سجل المعاملة داخل الكتلة فلا يمكن تعديل المعاملة ، أو العبث بها بعد أن يتم اقتراح هذه الكتلة بنجاح ، والتحقق من صحتها ، والالتزام بها في السلسلة ، وبالتالي، يتم ضمان اتساق البيانات في كل كتلة من كتل البلوك تشين [٢].

[1] - Mirko Koscina,op.cit.p19
[2] - Ibid

مع ذلك ليس من المستحيل تعديل التسجيل. في الواقع، إذا تم التوصل إلى إجماع على تعديل حالة السجل، فهذا يعني أن غالبية العُقد توافق على التحقق من صحة الكتل الجديدة من خلال العودة إلى الكتلة التي تسبق مرور السلسلة لتجاهلها[١].

وفى حال تمت الموافقة على التعديل فإن هذه التعديلات لا تؤدي لتعديل للمعاملة التي تمت(الكتلة) وإنما سيتم اضافة معاملة جديدة (كتلة) مما يعنى إجراء تغييرات على الإصدار الأصلي ، وتحديثا للسجل[٢] ، وهذا يعني أن المستخدمين اللاحقين سيرون نسخة محدثة بالكامل ، ولن يتمكنوا من رؤية سجل المعاملات[٣].

بالنسبة للهجوم على البلوك تشين ، فإنه الرغم من أن هذه التقنية تمنع عدة أنواع من الهجمات الضارة ، وتقلل من العديد من المخاطر المرتبطة بها، إلا أنها لا تقضي على جميع الهجمات[٤].

في مواقف معينة، يمكن للعُقد الخبيثة أن تتلاعب بسلسلة الكتل ، أو تدرج معاملات مزورة.

[1] - Claire Leveneur, op.cit.p.68 n° 80
[2] - Claire Leveneur ,op.cit.p.62
[3] - Houiqua Ismail,op.cit.p.8
[4] - Hajar Moudoud op.cit.p.4

١١ – حماية البيانات الشخصية عبر تقنية البلوك تشين

تجبر مؤشرات التجزئة العُقد الخبيثة على إعادة بناء السلسلة لتنجح في هجومها ، وإلا سيتم كشف العبث الذى قامت به، وهذا يعني أن هذه العُقد تحتاج إلى استثمار الكثير من الموارد لتنجح في هجومها[١].

فإذا حاول أحد الخصوم تعديل البيانات في أي كتلة تابعة للسلسلة، فيجب عليه تغيير مؤشرات التجزئة الخاصة بالكتل السابقة لإخفاء التلاعب[٢] ؛ لذلك يحتاج الخصم إلى تغيير جميع المؤشرات في جميع الكتل حتى الوصول إلى الكتلة الأولى (كتلة التكوين)، والتي يتم إنشاؤها بمجرد إنشاء النظام.

يمكن اعتبار الهجوم بمثابة عملية إعادة كتابة البلوك تشين ، من أجل المعاملات المناسبة. سيكون هذا هو الحال إذا قام ممثل خبيث بجمع ما لا يقل عن ٥١٪ من قوة الحوسبة الخاصة بالبلوك تشين. هذه الفرضية لم تحدث حتى الآن بالنسبة لأكبر سلاسل الكتل[٣].

---

[1] - Mirko Koscina,op.cit.p20.

[٢] - إن آلية التجزئة التي تمت مناقشتها لها متوسط عمر متوقع محدود، وفقًا للخبراء، بين ٢٠ و١٠٠ عام، وسيكون من الضروري بعد ذلك تحديث بروتوكول البلوك تشين ، باستخدام آلية تجزئة أخرى. Cédric Strub ,op.cit.p.28

[٣] – لتقويض البلوك تشين، سيكون من الضروري إفساد ٥١٪ من "عمال المناجم" حتى يتمكنوا بشكل جماعي من التحقق من صحة المعلومات الخاطئة، وهو أمر يكاد يكون مستحيلا نظرا لتفاوتهم – فهم موجودون بشكل عام في أركان العالم الأربعة ولا يعرفون بعضها البعض. وكلما زاد عدد العقد

تبلغ التكلفة المقدرة لهجوم بنسبة ٥١% على سلسلة كتل البيتكوين عدة مليارات من الدولارات[١] (بلغت التكلفة المقدرة في سبتمبر ٢٠١٨ أكثر من ١٨ مليار دولار، وفي مارس ٢٠٢١ أكثر من ٢٤ مليار دولار، في يوليو ٢٠٢٢ أكثر من ٣٤ مليار دولار)[٢]. بالتالي يمكننا قياس مدى فعالية النظام ، والذي يعتمد أمنه على التكلفة ، والوقت اللازمين لاختراق السلسلة ، بما لا يتناسب مع المكاسب المتوقعة ، لذلك، من المثير للاهتمام دائمًا إنفاق الطاقة الحاسوبية ؛ للتحقق من صحة المعاملات الصادقة والحصول على مكافآت مقابل ذلك[٣].

ب- تكلفة استخدام شبكة البلوك تشين:

مع زيادة عدد المستخدمين ، والمعاملات على شبكة البلوك تشين ، تحتاج العُقد إلى معالجة وتخزين المزيد من البيانات برسوم أعلى لتحقيق أقصى قدر من أرباحها.

الموجودة في البلوك تشين ، كلما أصبح خطر التلف ضئيلًا، وبالتالي فإن أمان البلوك تشين يصبح مرتفع للغاية.

Boris Barraud. Les blockchains et le droit. Revue Lamy Droit de l'immatériel, 2018, 147, pp.48-62 hal-01729646 p.3

[١] – تشير التقديرات، في عام ٢٠١٨، إلى أن تنفيذ "هجوم بنسبة ٥١%" على البلوك تشين الخاص بالبيتكوين، سيكلف مليار يورو للأجهزة فقط وما يقرب من ٤٧٥٠٠٠ يورو من الكهرباء لكل ساعة تشغيل. Thibaut Labbe. op.cit.p.17

[2] - Claire Leveneur op cit p.68

[3] - Claire Leveneur op cit p.69 n° 80

١١ – حماية البيانات الشخصية عبر تقنية البلوك تشين

يتم تعريف معالجة البيانات الشخصية وفق المادة الرابعة من اللائحة العامة لحماية البيانات الشخصية(GDPR) على أنها " أي عملية ، أو مجموعة من العمليات يتم إجراؤها على البيانات الشخصية، أو على مجموعات من البيانات الشخصية، سواء بوسائل آلية أم لا، مثل التجميع ،أو التسجيل ،أو التنظيم ،أو الهيكلة ،أو التخزين ، أو التكيف ، أو التغيير ،أو الاسترجاع ، أو الاستشارة ، أو الاستخدام ، أو الكشف عن طريق النقل ، أو النشر ، أو الإتاحة بطريقة أخرى ، أو المواءمة ، أو الجمع ، أو التقييد ، أو المحو ، أو التدمير" [١].

فالمعالجة فكرة يجب تفسيرها على نطاق واسع بموجب قانون حماية البيانات في الاتحاد الأوروبي.

فيما يتعلق بسلاسل الكتل ، فإن هذا الفهم الواسع جدًا لما يمكن اعتباره معالجة بيانات يدخل تحته الإضافة الأولية للبيانات الشخصية إلى دفتر الأستاذ الموزع، وتخزينها المستمر ، وأي معالجة إضافية (مثل أي شكل من أشكال تحليل البيانات ، وكذلك التوصل إلى توافق في الآراء بشأن تشكيل الحالة الحالية للشبكة).

[١] – قريب من ذلك المادة الأولى من قانون حماية البيانات المصري ١٥١ لسنة ٢٠٢٠.

وقد أكدت محكمة العدل الأوروبية أن معالجة البيانات الشخصية تشمل "أي عملية أو مجموعة من العمليات" يتم إجراؤها على البيانات الشخصية[١].

بالإضافة إلى ذلك، نظرًا لأن جميع طلبات المعاملات تتطلب رسومًا، فإن القائمين بالتعدين يمنحون الأولوية للمعاملات التي تدفع رسومًا أعلى ؛ لذلك، إذا كانت المعاملات بحاجة إلى التحقق بسرعة، فيجب على المستخدم دفع رسوم أعلى للحصول على الأولوية. كلما وافق المستخدم على دفع رسوم معاملات عالية، كلما تمت معالجتها بشكل أسرع.

غالبًا ما تفرض شبكات البلوك تشين حدًا صارمًا لحجم الكتلة للسماح للعُقد ذات الموارد المحدودة بالمشاركة في الشبكة، ومع ذلك، نظرًا للسعة المحدودة على السلسلة خلال فترات الذروة ، يضطر المستخدمون إلى دفع رسوم أعلى حيث يتنافسون لإدراج معاملاتهم في البلوك تشين[٢].

[1] - Case C-101/01 Bodil Lindqvist [2003] EU:C:2003:596, para 25.
[2] - Kahina Khacef op.cit.p.6

المطلب الثاني

البلوك تشين وقواعد البيانات التقليدية

سوف نستعرض في هذا المطلب مميزات تقنية البلوك تشين عن شبكة البيانات التقليدية ، ثم نتبع ذلك بالحديث عن التحديات الى تواجه البلوك تشين.

أولا : مميزات تقنية البلوك تشين

في البداية من المهم أن نعرف أن البلوك تشين ليس قاعدة بيانات بل شبكة ، وعلى هذه الشبكة يمكن للمستخدمين المعتمدين إدارة الإدخالات الجديدة ، وضبطها ، واستعادتها.

للتأكد من صحة جميع المعاملات، تؤكد العُقد (أعضاء الشبكة) موافقة جميع المشاركين. بمجرد التوصل إلى هذا الإجماع ، يتم حفظ التسجيلات بشكل دائم بسجلات مقاومة للتلاعب ، وبالتالي الحصول على الحصول على تكنولوجيا معلومات آمنة ، وموثوقة ، ودائمة ، تمنع المستخدمين ومسؤولي النظام من حذف التسجيلات في أي وقت[١].

[1] - Thibaut Labbe. op.cit.p.20.

تعمل تقنية البلوك تشين الآمنة بطبيعتها على إنشاء نسخة موحدة من الحقيقة التي يمكن مشاركتها بسهولة مع أعضاء الشبكة، مما يوفر الوقت ، ويقلل العمل الإضافي[١].

بمجرد إنشاء كتلة جديدة، وإرسالها إلى العُقدة، تضيفها العُقدة إلى نسختها من دفتر الأستاذ ، وتنقلها إلى العُقد النظيرة لها. تتحقق العُقد النظيرة مرة أخرى من صلاحية هذه الكتلة، وإذا كان الأمر كذلك ، تقوم بدمجها في السجل الخاص بها، وإرسالها مرة أخرى إلى أقرانها.

إذا حاولت كتلة غير صالحة التسجيل في دفتر الأستاذ ، فلن يتم التحقق من صحتها بواسطة معظم العُقد، وبالتالي لا تتم إضافتها إلى دفتر الأستاذ الخاص بها، ولا يتم نقلها إلى أقرانها ، ولذلك لا يتم تسجيل المعلومات في هذا السجل[٢].

من ناحية أخرى، تستخدم قاعدة البيانات التقليدية خادمًا مركزيًا يسمح للمستخدمين بتعديل كافة العناصر. على عكس شبكة البلوك تشين ، تؤدي التعديلات إلى إجراء تغييرات على الإصدار الأصلي ، وهذا يعني أن المستخدمين اللاحقين سيرون نسخة محدثة بالكامل ، ولن يتمكنوا من رؤية سجل المعاملات[٣].

[1] - Houiqua Ismail,op.cit.p.9-10.
[2] - Cédric Strub ,op.cit.p.22
[3] - Houiqua Ismail,op.cit.p.8

١١ - حماية البيانات الشخصية عبر تقنية البلوك تشين

هناك اختلاف رئيسي آخر بين شبكة البلوك تشين ، وقاعدة البيانات ، وهو أنه مع قاعدة البيانات يكون المسؤولون هم الذين لديهم السيطرة الكاملة. هذه الأشكال من السلطة مسؤولة عن تفويض الوصول ، ومنح الأذونات لمستخدميها.

إن البلوك تشين عبارة عن دفتر أستاذ مشترك يقوم بتخزين ونقل المعلومات حول المعاملات، وهو يشكل في حد ذاته قاعدة بيانات موزعة ، وهذا يعني أنه على عكس قاعدة البيانات التقليدية، فهي لا تقع في مكان واحد، ولكن في عدة مواقع في نفس الوقت[١].

تتيح تقنية البلوك تشين عمليات تبادل لا مركزية ، وآمنة، دون الحاجة إلى أطراف ثالثة موثوقة ، وهي عبارة عن سجلات منسوخة وموزعة، بدون هيئة تحكم مركزية، مؤمنة بالتشفير ، ومنظمة بواسطة كتل مرتبطة ببعضها البعض.

يتزايد الاهتمام بسلاسل الكتل، إلا أنه غالبًا ما يرتبط بقضايا التسويق. إن استخدام بعض التطبيقات المرتبطة بسلاسل الكتل ليس له ما يبرره دائمًا، ويمكن توفير الوظائف المميزة بوسائل شائعة/تقليدية. يبدو من الضروري إلقاء نظرة نقدية على البلوك تشين ، حتى لا نكون رهينة لبدعة ، لا تكون مصحوبة حقًا بابتكار قوي.

[1]- Cédric Strub , op.cit p.16

من أجل تحديد ما يمكن أن تقدمه تقنية البلوك تشين مقارنة بقواعد البيانات الحالية[١]، من الضروري طرح السؤال التالي: ما الذي لا تستطيع قاعدة البيانات التقليدية فعله؟ إذا لم نكن بحاجة مسبقًا إلى تكامل كبير للبيانات في سياق المشاركة القوية، كما أنه إذا كان تخزين البيانات على خادم مركزي لا يمثل مشكلة ، فالطرق التقليدية ستكون كافية، وفي هذه الحالة لن يكون للبلوك تشين أي فائدة حقيقية.

لذلك من الضروري تحديد النقاط التي تكون فيها البلوك تشين أكثر فائدة من قاعدة البيانات التقليدية، والعكس صحيح.

الميزة الأولى: عدم الوساطة

كما هو موضح أعلاه، فإن إحدى القيم العظيمة للبلوك تشين هي عدم الوساطة، فهي تسمح بمشاركة البيانات والمعاملات خارج حدود الثقة، دون الحاجة إلى مسؤول مركزي[٢].

في الأنظمة المركزية، يتم تبادل البيانات (أي المعاملات) من خلال طرف ثالث موثوق به. يمكن أن يؤدي هذا النهج المركزي إلى تكاليف إضافية فيما يتعلق بإدارة

[1]- Cédric Strub,op.cit.p.24-26.
[2]- Cédric Strub,op.cit.p.25 - Houiqua Ismail,op.cit.p.13.

وصيانة الموارد المركزية (الخوادم على سبيل المثال) ونقاط الضعف الأمنية واختناقات الأداء[١].

تعتمد تقنية البلوك تشين على تنفيذ بنية لا مركزية ، وهكذا، بدلًا من وجود هيئة مركزية تمتلك وحدها المستندات التي توزع نسخًا منها على العملاء، يمتلك كل كمبيوتر ملفات المجموعة.

تسمح تقنية البلوك تشين بإجراء المعاملات بشكل آمن وبدون هيئة تحكم مركزية؛ لذلك يتم تقديمها -كأداة تكنولوجيا المعلومات- على أنها في حد ذاتها تجسد الثقة اللازمة للمعاملات بين الأفراد الذين لا يعرفون بعضهم البعض مسبقًا[٢]، حيث تتيح تقنية البلوك تشين تنفيذ المعاملات ، ومنها على سبيل المثال عمليات نقل ملكية الأصول الرقمية غير القابلة للإلغاء ، دون هيئة مراقبة مركزية أو طرف ثالث موثوق به[٣].

فعلى سبيل المثال، في علاقة تعاقدية تتضمن التزامًا بدفع مبلغ من المال، يتطلب الدفع من أ إلى ب تدخل طرف ثالث، ج والذى سيكون بشكل عام أحد البنوك، مما

[1] - Houiqua Ismail op.cit p.17
[2] - Hajar Moudoud op.cit.p2
[3] - Claire Leveneur,op.cit.p.52

سيسمح بتحويل الأموال ، أما في إطار بروتوكول البلوك تشين ، يمكن التحقق من صحة الدفع تلقائيًا من قبل جميع المشاركين في البلوك تشين المذكور[١].

إذا كان الاستغناء عن مسئول مركزي يعني تقليل أوقات المعالجة، والتكاليف، ومخاطر الأخطاء ، والأعمال الضارة[٢]، فكيف يمكننا ضمان موثوقية نقل المعلومات عبر مكونات الكمبيوتر في الشبكة اللامركزية، إذا كان لا يوجد سلطة رقابية تصادق على أصل ، أو سلامة الرسائل ؟[٣]

المبدأ الأساسي للبلوك تشين هو أن الكود (البرنامج والبروتوكول المرتبط به) يتجاوز مفهوم الثقة ؛ لأنه موثوق في حد ذاته ، ويسمح للشخص بتحرير نفسه من فكرة الثقة في نظامه[٤].

في الواقع، "الثقة القائمة بين شخصين تعتمد فقط على الرياضيات، مما يسمح للمرء بالتحرر من أي طرف ثالث موثوق به ، سواء كان حكوميًا ، أو خاصًا".

على عكس الأنظمة المركزية التقليدية، فإن البلوك تشين عبارة عن دفتر أستاذ موزع يعمل_في شبكة لا مركزية، وبذلك فإن التكنولوجيا نفسها هي التي تصبح الطرف الثالث الضامن للتبادلات المبرمة بين مستخدميها.

---

[1] - Thibaut Labbe. op.cit.p.18
[2] - Cédric Strub ,op.cit.p.25
[3] - Claire Leveneur,op.cit.p.58 n° 64
[4] - Thibault Verblest, op.cit.p.51

ستكون تقنية البلوك تشين طرفًا ثالثًا جديدًا موثوقًا به ، ويمكن أن يحل محل الأطراف الثالثة التقليدية ، والمؤسسية الموثوقة[١]، وبالتالي، توفر طريقة لاستبدال هذه المؤسسات بقاعدة بيانات موزعة ، ومقفلة بواسطة التشفير الذكي، مستفيدة من القدرة المتزايدة لأنظمة الكمبيوتر ؛ لتوفير طريقة جديدة لاستبدال البشر بالرموز[٢].

الميزة الثانية : الأمان العالي

الميزة الثانية لقواعد البيانات التي تعمل بتقنية البلوك تشين هي الأمان العالي والتسامح الشديد مع الأخطاء ، حيث تقوم كل عُقدة بمعالجة كل معاملة[٣]، ولا توجد عُقدة واحدة مهمة لقاعدة البيانات بأكملها[٤].

يعد الأمان أحد أبرز خصائص البلوك تشين ، ففي الواقع يعد اختراق دفتر الأستاذ الموزع بين عدة آلاف من العُقد المنتشرة في جميع أنحاء العالم أكثر صعوبة من اختراق دفتر الأستاذ الموجود على خادم مركزي واحد[٥].

في البلوك تشين تتم مراقبة قاعدة البيانات النموذجية عن كثب بحثًا عن المشاكل، مع نسخ المعاملات على نظام نسخ احتياطي في موقع فعلي مختلف. إذا فشلت قاعدة

[1] - Claire Leveneur,op.cit.p.52.
[2] - Cédric Strub ,op.cit.p.25.
[٣] - توفر كل عقدة مستويات قصوى من التسامح مع الأخطاء، وتضمن عدم التوقف عن العمل، وتجعل البيانات المخزنة على البلوك تشين غير قابلة للتغيير إلى الأبد ومقاومة للرقابة
Houiqua Ismail,op.cit.p.17
[4] - Cédric Strub ,op.cit.p.25
[5] - Cédric Strub ,op.cit.p.27.

البيانات، فسيتم نقل النشاط تلقائيًا إلى النسخة الاحتياطية. يعد نظام النسخ الاحتياطي هذا مكلفًا للصيانة، وقد يكون من الصعب تحقيق التحول من قاعدة بيانات إلى نسخة احتياطية[١].

يضمن الجانب اللامركزي أمان المعلومات والتبادلات المسجلة في تاريخ البلوك تشين. فبما أن جميع المستخدمين لديهم نسخة من كل معاملة، فإن خطر الهجوم السيبراني يكون أقل بكثير[٢].

عند استخدام البلوك تشين تكون العُقد (وبالتالي النسخ الاحتياطية) متعددة، وكذلك مواقعها الجغرافية. كل ذلك بمعدات كلاسيكية ، وغير مكلفة. ترتبط هذه العُقد ارتباطًا وثيقًا ببعضها البعض، حيث تتشارك المعاملات على أساس نظير إلى نظير. إذا فشلت عُقدة واحدة أو اثنتين بشكل كامل، فلن يتم الشعور بالتأثير، حيث لا يزال هناك العديد من العُقد المتاحة[٣].

في الحقيقة فإن اللامركزية تعمل على تعزيز أمن النظام ، حيث يمكن أن يؤدي فشل هيئة مركزية ، أو فسادها إلى تدمير شبكة بأكملها، أما النظام الذي تتم إدارته بواسطة

[1] - Cédric Strub ,op.cit.p.25
[2] - Houiqua Ismail,op.cit.p.16
[3] - Cédric Strub ,op.cit.p.25

١١ - حماية البيانات الشخصية عبر تقنية البلوك تشين

البلوك تشين باعتباره نظام لا مركزي يجعل من الممكن تجنب هذه المخاطر حيث يتطلب فشل نصف أعضائه (العقد) على الأقل ليتم تدميره[١].

إن مميزات البلوك تشين تجعلها أداة قوية سواء بالنسبة للمصنعين، مما يسمح لهم بالاعتماد على سلامة البيانات، وأمنها، أو للفرد ، وأخيرًا من أجل الصالح العام .

يسمح الثبات بحماية البيانات، وتسمح اللامركزية بالمشاركة الهائلة للبيانات، وهي خصائص أساسية للبحث.

وقد حدا ذلك بدولة إستونيا وخى البلد يعتبر الدولة الأكثر رقمية في العالم بأن تستخدم حاليًا تقنية البلوك تشين في العديد من المجالات[٢].

من خلال استخدام تقنية البلوك تشين ، تعمل إستونيا، وهي أول دولة تستخدم تقنية البلوك تشين على المستوى الوطني، على تطوير حلول الهوية الإلكترونية، والصحة الإلكترونية و مشاركة البيانات الصحية ، والعدالة الإلكترونية.

توفر هذه الحلول وقتًا ثمينًا ، وبخاصة في معالجة الطلبات الخاصة بالعدالة ، حيث تعد إستونيا واحدة من البلدان التي لديها أسرع الإجراءات القانونية في العالم ، وحتى

[1] - Thibaut Labbe. op.cit.p.18-20
[2] - Cédric Strub ,op.cit.p.49.

الذهاب إلى أبعد من ذلك حيث معالجة الأصوات الانتخابية ، مما حدا ب٤٤% من الإستونيين من استخدام الإنترنت في التصويت في الانتخابات[١].

ثانيا: التحديات التي تواجه البلوك تشين

لقد تطورت تقنية البلوك تشين بسرعة في السنوات القليلة الماضية، وفي الوقت الحالي من الممكن العثور على أنواع مختلفة من هياكل شبكة البلوك تشين. ولدت هذه البنى الجديدة بسبب حالات الاستخدام ، والأنظمة البيئية المختلفة حيث يمكن تنفيذ الخدمات القائمة على البلوك تشين[٢].

ومع ذلك فإن البلوك تشين يواجه العديد من التحديات ، فحتى لو بدا أن البلوك تشين يضمن سلامة معاملاته ، فهو ليس خاليًا من العيوب.

أحد أكبر التحديات، إن لم يكن التحدي الأكبر، لتقنية البلوك تشين هو مدى قدرته على التعامل مع الزيادة في عدد المعاملات ، خاصة وأن البروتوكول المستخدم في العمل – بخاصة البيتكوين– لمصادقة البيانات بطئ جدا ويستهلك الكثير من الطاقة الضرورية للحفاظ على السجل[٣].

[1] - Solutions - Building blocks of e-estonia [Internet]. e-Estonia. https://e-estonia.com/solutions/
[2] - Mirko Koscina,op.cit.p.21
[3] - Mustapha Mekki,op.cit. n°12- Houiqua Ismail,op.cit.p.16

١١ - حماية البيانات الشخصية عبر تقنية البلوك تشين

على سبيل المثال، حتى عام ٢٠١٧، كانت سلسلة بلوك تشين البيتكوين تسمح فقط بالتحقق من صحة ٤ معاملات في الثانية، وفى عام ٢٠٢٠ كانت تسمح بحوالي عشرين معاملة ، وتعد سرعة المعالجة هذه منخفضة مقارنة بما تسمح به قواعد البيانات المركزية.

كما أدى هذا التحدي إلى البحث عن استجابات تكنولوجية محتملة وأدى إلى ابتكارات لم تنضج بعد، مثل الربط بين العديد من سلاسل الكتل ذات الوظائف المختلفة والمتكاملة ، وكذلك استخدام قواعد البيانات التقليدية المرتبطة بسلسلة الكتل[١].

كذلك فإن كل عُقدة توفر مستويات قصوى من التسامح مع الأخطاء، وتضمن عدم التوقف عن العمل، وتجعل البيانات المخزنة على البلوك تشين غير قابلة للتغيير إلى الأبد ، كما أنها تكون مقاومة للرقابة ، لكن هذه الإجراءات تستهلك الكهرباء والوقت عندما تكرر كل عُقدة تحقيق الإجماع[٢].

كذلك فإن التحقق من التوقيع هو تحدي أخر تواجهه تقنية البلوك تشين ، لأنه يجب توقيع كل معاملة باستخدام نظام تشفير، وهناك حاجة إلى قوة حاسوبية كبيرة لعملية حساب التوقيع ، وهذا هو سبب ارتفاع استهلاك الطاقة[٣].

---

[1] - Cédric Strub ,op.cit.p.27
[2] - Houiqua Ismail,op.cit.p.7
[3] - Houiqua Ismail,op.cit.p.7

بالإضافة إلى ذلك، فإن قابلية التوسع في البلوك تشين محدودة ، وتنشأ هذه المشكلة عندما يزداد عدد العُقد في البلوك تشين، لأن كل عُقدة يجب أن تقوم بتخزين وتنفيذ المهام الحسابية للتحقق من صحة كل معاملة.

تحتفظ البلوك تشين بتاريخ متزايد باستمرار من المعلومات المطلوبة لتحقيق الإجماع ، وتوفير الأمان. بالإضافة إلى ذلك، تزداد تكاليف التخزين جنبًا إلى جنب مع عدد المعاملات، مما قد يشكل عائقًا يحد من قابلية التوسع في البلوك تشين ويعد تحديًا أمام الحصول على اعتماد واسع النطاق.

تعتمد بيتكوين ، وايثروم على نظام النسخ المتماثل الكامل، مما يعني أن كل عُقدة في الشبكة (العُقدة المسؤولة عن التحقق من الصحة) تقوم بتخزين البلوك تشين التاريخي بأكمله. تتحقق العُقد من صحة المعاملة الجديدة عن طريق التحقق من الحالة المسجلة ثم الاحتفاظ بكل معاملة. ويتحمل هذا النسخ ما يصل إلى ٤٩% من العُقد الضارة، مما يسمح بمستوى عالٍ من الأمان؛ ومع ذلك، فإن هذا يحد بشدة من كفاءة التخزين وقابلية التوسع[١].

يعيق هذا التصميم قابلية التوسع في البلوك تشين ؛ نظرًا لأن هذه العُقد تخزن البلوك تشين من الكتلة الأولى وستستمر في تلقي معلومات جديدة لتخزينها[٢].

[1] - Kahina Khacef, op.cit. P.5
[2] - Ibid.

١١ - حماية البيانات الشخصية عبر تقنية البلوك تشين

إن اللامركزية في البلوك تشين محدودة بحجم سجل المعاملات ، ومن المستحيل أن يكون لدى البلوك تشين اللامركزي قاعدة بيانات تحتوي على تاريخ من المعاملات يمتد لسنوات، حيث سيكون كبيرًا جدًا بحيث لا يمكن تخزينها ، ومزامنتها عبر شبكة لا مركزية.

يمكن أن يصبح هذا مكلفًا للغاية مع نمو سجل المعاملات لفترة أطول، مما يحد من استخدام سلاسل الكتل اللامركزية للتطبيقات التي تتطلب عددًا كبيرًا من المعاملات ، وفترة طويلة من الزمن [١].

إضافة إلى ذلك، هناك مشكلة اللامركزية حيث يتم تخزين سجل المعاملات فقط في منتجي الكتل ، وهم عدد قليل من العُقد – من بين آلاف أو ملايين العُقد في البلوك تشين– الذين يمكنهم الوصول إلى سجل المعاملات؛ لذلك من الصعب القول أن سلسلة الكتل هذه لا مركزية. كما أن المشكلة الكبرى للبلوك تشين ستكون في حال حدث شيء ما لهذه المجموعة القليلة من العُقد التي تخزن سجل المعاملات.

كذلك فإن العديد من المشاريع تستخدم الحوسبة السحابية لتخزين سلسلة الكتل الخاصة بها لزيادة قابلية التوسع ، على سبيل المثال، Solana [٢] وEthereum،

---

[1] - Kahina Khacef op.cit.p.17

[٢] - تمتلك Solana أكثر من ١٧٠٠ أداة تحقق، ولكن تتم معالجة جميع المعاملات بواسطة مجموعة أصغر بكثير مكونة من ١٥٠ أداة تحقق، بالإضافة إلى ذلك، تستخدم سلسلة

والتي يتم تخزينها في الحوسبة السحابية بسبب أحجام الكتل الضخمة، وبالتالي التضحية باللامركزية ، مما أثار معضلة ثلاثية معروفة جيدًا تدعي أنه لا يوجد نظام دفتر أستاذ لامركزي يمكنه تحقيق الأمان، اللامركزية، و قابليته للتوسع[١].

يمكن أن يكون للحلول السطحية مثل زيادة حجم الكتلة أو الإنتاجية لتحسين قابلية التوسع للبلوك تشين تأثير سلبي ؛ لأنها تؤدي إلى تدهور أمان البلوك تشين ، وتؤدي إلى عدم الاتساق ، لذلك فإن الموازنة بين إنتاجية وسعة البلوك تشين مع ضمان الأمان أمر ضروري للتطوير المستقبلي للبلوك تشين [٢].

كذلك من ضمن التحديات التي تواجه البلوك تشين مواجهة مخاطر الهجوم التي تقع على الواجهات ، فإذا كان اختراق دفتر الأستاذ الموزع بين عدة آلاف من العُقد المنتشرة في جميع أنحاء العالم أكثر صعوبة من اختراق دفتر الأستاذ الموجود على خادم مركزي واحد. مع ذلك، حتى لو بدا أن البلوك تشين يضمن سلامة معاملاته، فهو ليس خاليًا من العيوب.

الكتل(Hetzner وOVHCloud) هذه خدمات الحوسبة السحابية لتخزين سلسلة الكتل الخاصة بها وهذا يجعل العملية مركزية. Kahina Khacef op.cit.p.18

[1] - Kahina Khacef op.cit.p.6

[2] - Hajar Moudoud op.cit.p.3

إذا كان النطاق المتزايد لسلسلة الكتل وتشتتها يزيد من صعوبات تعديل الكود الخاص بها أو إدخال معاملات احتيالية. مع ذلك فإن معظم عمليات الاختراق المسجلة لا تتعلق بالبروتوكول ولا بالبلوك تشين نفسه، بل بالواجهات المصنوعة معه.

على سبيل المثال، إذا تم ربط البلوك تشين بتطبيق هاتف ذكي، فستستهدف الهجمات هذا التبادل، وفي هذه الفترة الزمنية البسيطة يمكن للمستخدم الخبيث التسلل إلى البيانات وتعديلها[١].

كذلك فإن البلوك تشين العام المفتوح لا يتوفر به أي حوكمة ، وبالتالي لا توجد وسيلة للتحكم أو العقوبة. فمع احترام عمل البروتوكول، يمكن للمستخدم الضار أن يحاول القيام بأعمال احتيالية دون المخاطرة بعقوبة[٢] ، مستعينا في ذلك بالاسم المستعار الذي يهيمن على سلاسل الكتل العامة ، والذى يمكن أن يسهل الاحتيال ، وغسيل الأموال ، وتمويل الإرهاب[٣].

كذلك من الممكن الهجوم على البروتوكول نفسه ، حيث يتم العثور على عيوب في كود بروتوكول البلوك تشين ، مع قدرة التقدم في الحوسبة على المساعدة في اكتشاف العيوب التي لم يتم تحديدها من قبل[٤].

[1] - Cédric Strub ,op.cit.p.27
[2] - Ibid
[3] - Mustapha Mekki,op.cit. n° 12
[4] - Cédric Strub ,op.cit.p.28

بالإضافة إلى ذلك فإن التشفير المرتبط بتقنية البلوك تشين مبالغ فيه ، حيث إن المفتاح الخاص لاستخدام البلوك تشين الخاص بالبيتكوين هو سلسلة مكونة من ٥٨ حرفًا أبجديًا رقميًا. على عكس البنك الذي لديه حسابات ، وأرقام حسابات ، ومصرفي قادر على العثور على أرقام الحسابات المفقودة ، في حين أن فقدان المفتاح الخاص يؤدي إلى خسارة دائمة لعملات البيتكوين المقابلة[١].

فغالبًا ما يشير التشفير المرتبط بتقنية البلوك تشين إلى أنها تقنية آمنة، وبدون التشكيك في هذه الفكرة ، يجب علينا قبل كل شيء أن ندرك أن الأمن ليس مجرد تكنولوجيا. فمن الثابت بشكل عام أنه لا يوجد أمن دون إشراف قانوني، وقبل كل شيء، دون استجابة إدارية.

فنظرًا لعدم وجود رابط معتمد بين الشخص الطبيعي الذي يحمل العنوان العام وتوقيعه المشفر، لا يمكن تنفيذ أي إجراء تقليدي (تقني أو قانوني) لاستعادة الأموال المحظورة في محفظة العملة المشفرة الخاصة به ، والمحمية بالتشفير غير المتماثل[٢]، ولن يتمكن سوى الشخص الذي أنشأ عنوانه العام من العثور على رموز الوصول باستخدام

[1] - Mustapha Mekki,op.cit. n° 11
[2] - Claire Leveneur, op.cit.p.63 n° 73

عبارة مكونة من اثنتي عشرة كلمة ("تسمى العبارة الأولية") والتي تم إنشاؤها أثناء إنشاء محفظة التشفير الخاصة به[١].

ومن الأمثلة الواقعية على ذلك حالة الكندي جيرالد دبليو كوتن، الذي كان على رأس سلسلة بلوك تشين بقيمة ١٨٠ مليون دولار أمريكي ، والذي توفي وهو يحمل معه رموز الوصول التي لم تكن لدى أي شخص آخر، ولم يكن هناك أي خطة طوارئ أو أية وثائق تشرح تدابير الطوارئ.

في الحقيقة إن الأمن ليس مستقلا ، بمعنى أنه لا يمكن النظر إليه في إطار الفهم التكنولوجي وحده.

ففي حالة الكندي جيرالد دبليو كوتن تكمن الإثارة في هذه القضية من أنه تم الإعلان عنها عن غير قصد تقريبًا أثناء إجراءات إعلان إفلاسه ، حيث جاءت أرملة هذا المليونير للإدلاء بشهادتها بشأن اختفاء زوجها[١].

---

[١] – العبارة الأولية أو عبارة الاسترداد الأولية هي عبارة احتياطية تتكون من قائمة من الكلمات التي تخزن جميع المعلومات اللازمة لاسترداد أموال بيتكوين على السلسلة.
عادةً ما يقوم برنامج المحفظة بإنشاء عبارة أولية ويطلب من المستخدم كتابتها على الورق .إذا تعطل جهاز الكمبيوتر الخاص بالمستخدم أو أصبح محرك الأقراص الثابتة الخاص به تالفًا، فيمكنه تنزيل برنامج المحفظة نفسه مرة أخرى واستخدام النسخة الاحتياطية الورقية لاستعادة عملات البيتكوين الخاصة به.
يمكن لأي شخص آخر يكتشف هذه العبارة أن يسرق عملات البيتكوين، لذلك يجب الحفاظ عليها آمنة مثل المجوهرات أو النقود؛ لذلك يجب ألا تتم كتابته في أي موقع ويب."
Claire Leveneur, op.cit.p.63 n° 73

بالإضافة إلى ذلك فإن بعض الجهات الفاعلة تحذر من مخاطر جديدة خاصة بالبلوك تشين ، ولا سيما النشر المتعمد لمعلومات كاذبة[٢]. فعلى الرغم من أن البلوك تشين يمكن أن يضمن ثبات البيانات في السلسلة ، وتحديد التحولات، إلا أن البيانات الغير مشروعة ، أو البيانات التي تصل تالفة ، أو مزورة في البلوك تشين تظل على حالها ؛ وذلك لأن البلوك تشين لا يمكنه الوصول إلى البيانات والخدمات الواقعية للتحقق من موثوقية البيانات [٣]، كما أنه لا يمكن محوها، بسبب الخاصية الثابتة لتقنية البلوك تشين[٤].

وقد أظهرت دراسة نشرها باحثون ألمان من جامعة آخن في مارس ٢٠١٨ ، والتي كشفت أن سلسلة كتل البيتكوين تحتوي على عدد معين من الملفات ، أو روابط لملفات غير تابعة للكتلة. هذه الملفات لها الطبيعة المالية ، والجمع بين الوثائق الخاضعة للملكية الفكرية ، والمعلومات الخاصة ، والمحتوى الحساس ، وبرامج المساعدة على التزييف ، وكذلك الروابط إلى المواقع الإباحية للأطفال[٥].

[1] - Vincent Gautrais, Les sept péchés de la blockchain : éloge du doute !Dalloz IP/IT 2019 p.432 n° 2
[2] - Cédric Strub ,op.cit.p.29
[3] - Hajar Moudoud op.cit.p.4
[4] - Cédric Strub ,op.cit.p.29
[5] - Ibid.

كذلك فإن سلسلة الكتل الخاصة ، على عكس سلسلة الكتل العامة ، يمكن تزويرها بسهولة أكبر ؛ نظرًا للعدد الصغير من القائمين بالتعدين الذين يمكنهم الاتفاق فيما بينهم على المعلومات التي سيتم دمجها في سلسلة الكتل.

والحقيقة أن هذا النوع من البلوك تشين منتقد ؛ لأنه يشكك في المبادئ التأسيسية لهذه التكنولوجيا، وهي النزاهة ، واللامركزية[1].

[1] - Audrey SIDE et al. op.cit p.3

المبحث الثاني
البيانات الشخصية في البلوك تشين

يُظهر تاريخ حماية البيانات أن اختراعها يرتبط ارتباطًا وثيقًا بتصور الحوسبة في الستينيات على أنها شيء خطير، فقد تمت مقارنة الكمبيوتر بالأسلحة النووية من قبل نواب الشعب الأمريكي ، حيث إنهم كانوا على قناعة بأن حجم المشكلة التي تواجههم الآن تشبه التغيرات التي حدثت في حياتهم الوطنية مع بزوغ فجر العصر النووي.

كانت وجهة نظرهم أن التخزين المحتمل وإعادة تجميع المعلومات الشخصية في المستقبل سيضرب أيضًا جوهر مفهومهم الديني(اليهودي المسيحي) المتمثل في "التسامح والنسيان"؛ لأن الكمبيوتر لا يغفر ولا ينسى[١].

إن قوانين الخصوصية لم تكن مهمة كما هي اليوم ، ففي الوقت الحاضر تنتقل البيانات حول العالم عبر شبكات بلا حدود. أصبح مفهوم البيانات الشخصية شائعًا، حيث سهلت تكنولوجيا المعلومات والإنترنت جمع البيانات الشخصية ؛ مما أدى إلى سوق مربحة[٢]، ويبدو ذلك جليا من خلال قيام مواقع الشبكات الاجتماعية بإعادة بيعها

[1] - Julien Rossi. Qu'est-ce que le droit à la protection des données à caractère personnel ?. Geopolitics of Risk Working Papers, 2018, Février . hal. p.10.

[٢] - انظر تقرير إيرادات الإعلانات على الإنترنت.
https://www.iab.com/wp-content/uploads/2019/10/IAB- HY19-Internet-Advertising-Revenue-Report.pdf(cit. on p. 11.)

للمعلنين من أجل استهداف احتياجات المستهلكين بشكل أفضل بهدف تزويدهم بإعلانات أكثر ملاءمة[١].

يختلف تعريف البيانات الشخصية باختلاف البلدان، وبما أن السوق عبر الإنترنت يعتمد على البيانات الشخصية، فمن الصعب تنظيم هذا السوق.

لدى الاتحاد الأوربي اللائحة العامة لحماية البيانات "GDPR" ، وتوجيهات الخصوصية الالكترونية[٢] لتحديد البيانات الشخصية ، والتي تعد الأخيرة المدخل لتطبيق اللائحة العامة لحماية البيانات"GDPR". فإذا كانت معالجة البيانات تتعلق بالبيانات الشخصية فقط ، فسيتم تطبيق هذه اللائحة وفقا للمادة الرابعة منها.

المشرع المصري بدوره قد أدرك خطورة الاعتداء على الاعتداء على الخصوصية والبيانات الشخصية ؛ مما حدا به لإصدار قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠ ، ولا شك في أهمية هذه الخطوة لما لذلك من أثر في تحقيق الاستقرار المعلوماتي وتنظيم عمليات نقل ومعالجة البيانات الشخصية عبر الحدود ، وبما يسهم في التنمية الاقتصادية ، وحماية الاستثمارات ، وتحقيق المعايير الدولية في مجال

[١] – محمد أحمد المعداوي ، حماية الخصوصية المعلوماتية عبر مواقع التواصل الاجتماعي ، دراسة مقارنة ، مجلة كلية الشريعة والقانون بطنطا العدد ٣٣ الجزء الرابع ديسمبر ٢٠١٨ ص ١٩٣٦

[٢] - يعد توجيه الخصوصية الإلكترونية لعام ٢٠٠٢ أداة قانونية مهمة للخصوصية في العصر الرقمي، وبشكل أكثر تحديدًا سرية الاتصالات والقواعد المتعلقة بالتتبع والمراقبة.
https://ec.europa.eu/digital-single-market/en/news/eprivacy- directive(cit. on p. 11.)

حماية البيانات الشخصية من خلال القواعد والمعايير التي يفرضها ويباشر الاشراف عليها مركز حماية البيانات المنشأ لهذا الغرض[١].

في هذا المبحث سوف نتناول أولا البيانات الشخصية وصورها في المطلب الأول ، ثم نتناول البيانات الشخصية في البلوك تشين في المطلب الثاني.

المطلب الأول

ماهية البيانات الشخصية[٢].

البيانات الشخصية هي أي معلومات تتعلق بشخص طبيعي محدد أو يمكن تحديد هويته. يمكن تحديد هوية الشخص إذا كان من الممكن التعرف عليه بشكل مباشر أو غير مباشر، خاصة بالرجوع إلى معرف مثل الاسم ، ورقم التعريف ، وبيانات الموقع ومعرف الإنترنت وما إلى ذلك[٣].

[١] - خالد سويلم محمد سويلم ، الحماية القانونية للبيانات الشخصية الالكترونية ، دراسة مقارنة ، المجلة القانونية. مجلد ١٤، العدد ٦ (٢٠٢٢) ص ١٩٠٥

[2]- Supriya Adhatarao. On GDPR Compliant Data Processing. Cryptography and Security [cs.CR]. Université Grenoble Alpes [2020-..], 2021

[٣]– في فرنسا وعلى المستوى الوطني، المادة ٢ من القانون رقم ٧٨–١٧ الصادر في ٦ يناير ١٩٧٨ المتعلق بمعالجة البيانات والملفات والحريات(المعروف بقانون حماية البيانات) والذي يحدد البيانات الشخصية بأنها "أي معلومات تتعلق بشخص طبيعي محدد أو يمكن التعرف عليه، بشكل مباشر أو غير مباشر، بالإشارة إلى رقم التعريف أو إلى عنصر أو أكثر خاص به.

١١ - حماية البيانات الشخصية عبر تقنية البلوك تشين

على المستوى الأوروبي، ينص القانون العام لحماية البيانات والمعروف باسم اللائحة العامة "GDPR"[١]، باستخدام التعريف الوارد في التوجيه الأوروبي لعام ١٩٩٥[٢]، تقرر تقرر المادة الرابعة أن البيانات الشخصية تتوافق مع " أي معلومات تتعلق بشخص طبيعي محدد أو يمكن تحديد هويته (يشار إليه باسم "صاحب البيانات) هذه مجرد بيانات تتعلق بالأشخاص الطبيعيين وليس لها أية علاقة بالكيانات الاعتبارية.

تم تحديد أن "الشخص الطبيعي الذي يمكن تحديد هويته" هو شخص طبيعي يمكن تحديد هويته، بشكل مباشر أو غير مباشر، لا سيما بالرجوع إلى معرف، مثل الاسم أو رقم التعريف ، أو بيانات الموقع ، أو معرف عبر الإنترنت ، أو إلى أحد عناصر

كذلك تعريف CNIL (اللجنة الوطنية لتكنولوجيا المعلومات والحريات) والتي حددتها بأنها "أي معلومات تتعلق بشخص طبيعي من المحتمل أن يتم التعرف عليه، بشكل مباشر أو غير مباشر، على سبيل المثال: اسم، صورة، بصمة إصبع، عنوان بريدي، عنوان بريد إلكتروني، رقم هاتف، رقم ضمان اجتماعي، رقم داخلي، عنوان IP، معرف اتصال الكمبيوتر، تسجيل صوتي، إلخ. »
https://www.cnil.fr/fr/cnil-direct/question/une-donnee-caractere-personnel-cest-quoi.

[1] - Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, dit« RGPD » règlement général sur la protection des données)

[٢] – قريب من ذلك المادة الأولى من قانون حماية البيانات المصري رقم ١٥١ لسنة ٢٠٢٠.

فيما يتعلق بتعريف "البيانات الشخصية"، الواردة في التوجيه ٤٦/٩٥، ذات صلة بموجب اللائحة العامة لحماية البيانات (GDPR) التي اعتمدت هذا التعريف حرفيًا.

Cécile de Terwangne et Élise Degrave Avec la collaboration d'Antoine Delforge et de Loïck Gérard,La protection des données à caractère personnel en Belgique,Manuel de base, ISBN 978-2-509-03505-9 D/2019/8132/88. p.15

أكثر تحديدًا خاصة بهويتهم الجسدية أو الفسيولوجية أو الجينية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية[١].

يعكس هذا التعريف رغبة المشرع الأوروبي في تعريف مفهوم "البيانات الشخصية" بشكل واسع يغطي جميع المعلومات التي يمكن ربطها بشخص ما[٢].وعلى ذلك امتدت الحماية لتشمل المعلومات المرتبطة بالتقنيات الحديثة والتي تحدد شخصا بشكل غير مباشر ولم تقتصر على المعلومات التي تحدد هوية الشخص بشكل مباشر مثل اسمه بل شملت عنوان البريد الالكتروني ، ورقم الهاتف ، ورقم بطاقة الائتمان ، أو بيانات بيومترية[٣].

ويترتب على هذه التعريفات أن البيانات الشخصية تتوافق مع المعلومات التي تحدد هوية الشخص الطبيعي أو تسمح بالتعرف عليه ، والتي تشتمل على جميع أنواع المعلومات سواء أكانت المعلومات العامة ، أو الخاصة ، أو المهنية ، أو التجارية ، أو المعلومات الموضوعية ، أو الذاتية.

---

[1] - Sarah Sadik. La protection des données dans les contrats de cloud computing. these,. Université de Perpignan, 2023.p.20

[2] - Groupe 29, Avis 4/2007 sur le concept de données à caractère personnel, p. 4 ; dans De Terwangne C. et Rosier K., Le Règlement général sur la protection des données (RGPD / GDPR), Analyse approfondie, 1re édition 2018, Larcier

[٣] – كافي زغير شنون ، الحماية القانونية للبيانات الشخصية الالكترونية ، مجلة الرافدين للحقوق ، المجلد ٢٣العدد٨٤ السنة ٢٥– سبتمبر ٢٠٢٣ ص ٢٩٨

١١ - حماية البيانات الشخصية عبر تقنية البلوك تشين

بالنظر إلى حماية الخصوصية وحماية البيانات الشخصية الموجودة على التوالي في المادتين السابعة والثامنة[١] ، سنجد أنهما ليسا نفس الشيء من وجهة نظر قانون الاتحاد الأوروبي، وخاصة ميثاق الحقوق الأساسية.

كما أن محكمة العدل التابعة للاتحاد الأوروبي (CJEU) أشارت إلى أن مفهومي البيانات الشخصية ، والبيانات المتعلقة بالحياة الخاصة ليسا متماثلين[٢].

ومع ذلك فإن هذه المحكمة لم تقترح مبدأ واضح يشرح العلاقة بين المادة السابعة من الميثاق الأوروبي للحقوق ، الذي يحمي الحق في الخصوصية، والمادة الثامنة من نفس الميثاق، التي تحمي الحق في حماية البيانات الشخصية[٣].

وفق ما سبق فإننا يمكننا القول بأن البيانات الشخصية ليست هي المعلومات المتعلقة بالحياة الخاصة للشخص فقط ؛ وذلك لأن الحق في حماية البيانات الشخصية لا

---

[١] – تنص المادة السابعة من الميثاق الأوروبي للحقوق الأساسية على أن " لكل فرد الحق في احترام حياته الخاصة ، والعائلية ، ومنزله ، واتصالاته."

وتنص المادة الثامنة على أنه " ١. لكل فرد الحق في حماية البيانات الشخصية المتعلقة به.

٢- يجب معالجة هذه البيانات بشكل عادل، لأغراض محددة وعلى أساس موافقة صاحب البيانات ، أو أي أساس مشروع آخر ينص عليه القانون. لكل شخص الحق في الوصول إلى البيانات المجمعة عنه وتصحيحها.

٣. يخضع الالتزام بهذه القواعد لرقابة هيئة مستقلة.

[2] - CJUE 16 juillet 2015 « ClientEarth contre EFSA » Aff. C-615/13 P, pt. 32

[3] - Julien Rossi. Op cit p.1

يخدم دائما حماية الخصوصية وفقط[١] ؛ ذلك أن قواعد حماية البيانات الشخصية تتجاوز حماية المفهوم العام للحق في احترام الحياة الخاصة والعائلية ، حيث هناك مبررات مختلفة لهذا الحق المكفول في المادة الثامنة من ميثاق الحقوق الأساسية للاتحاد الأوروبي، أحد هذه المبررات التي تظهر بشكل منتظم هو إدراك الخطر الناشئ عن حوسبة المجتمع[٢].

يشمل مفهوم البيانات الشخصية أي نوع من المعلومات ، وبالتالي، فهو يغطي المعلومات الخاصة، التي تتم مشاركتها من قبل مجموعة مقيدة، أو حتى المعلومات السرية تمامًا، و أيضًا المعلومات التي تم بثها أو نشرها[٣].

فيما يتعلق **بالمعلومات العامة** : هي تلك البيانات التي يمكن للجمهور الوصول إليها من خلال الشبكات التواصل الاجتماعي ، أو مواقع الويب ، أو السجلات العامة الأخرى، وما إلى ذلك [٤]، فإن نشر تلك البيانات ، وفقا لمحكمة العدل الأوربية ، أي

[١] – تشمل عبارة "البيانات الشخصية" المعلومات المتعلقة بالحياة الخاصة والعائلية للشخص الطبيعي، بالمعنى الضيق للكلمة، ولكنها تشمل أيضًا المعلومات المتعلقة بأنشطته، مهما كانت، وكذلك تلك المتعلقة بعلاقاته المهنية والعملية والاقتصادية ، أو السلوك الاجتماعي، وبالتالي يتعلق الأمر بالمعلومات المتعلقة بالأشخاص الطبيعيين، بغض النظر عن وضعهم أو قدراتهم (كمستهلكين، مرضى، موظفين، عملاء، وما إلى ذلك).
Groupe 29, Avis 4/2007 op cit, p. 7

[2] - Julien Rossi. Op.cit.p.10

[3] - Cécile de Terwangne et al., op cit.p.15

[4] - Cécile de Terwangne et al., op cit.p.15- Sarah Sadik op cit.p.21.

جعلها معروفة أو متاحة لعدد غير محدد من الأشخاص، ليس معناه أنها لم تعد تستفيد من الحماية. وبعبارة أخرى، لا مجال لتجريد البيانات من أي حماية بمجرد نشرها بأي شكل من الأشكال، سواء على شبكة الإنترنت ، أو في إحدى الصحف على وجه الخصوص[١].

فيما يتعلق **بالبيانات المتعلقة بالحياة المهنية** للفرد أو أنشطته التجارية فإنها تعد من ضمن البيانات الشخصية الخاضعة للحماية ، طالما أنه من الممكن ربطها بشخص معين[٢]، وقد أشارت المحكمة الابتدائية للاتحاد الأوروبي إلى أن "ألقاب وأسماء المسؤولين الأوروبيين والأشخاص الذين تظهر أسماؤهم في قوائم مسابقات التوظيف المنظمة محفوظة من قبل الاتحاد الأوروبي تشكل بيانات شخصية"[٣].

وقد أوضحت السوابق القضائية لمحكمة العدل الأوربية أنه "لمعرفة ما إذا كنا في وجود بيانات شخصية، لا يتعلق الأمر بتحديد ما إذا كانت المعلومات تقع ضمن نطاق الحياة الخاصة أم لا، ولكن فقط لتحديد ما إذا كانت المعلومات تتعلق بشخص محدد ، أو شخص يمكن التعرف عليه ؛ لذلك فإن الأسماء الأولى والأخيرة

[1] - CJUE, 16 décembre 2008, affaire n° C-73/07, Tietosuojavaltuutettu c. Satakunnan markkinapörssi oy et Satamedia oy
[2] - Cécile de Terwangne et al., op cit.p.15
[3] - TPIUE, 7 juillet 2011, affaire n° T-161/04, Gregorio Valero Jordana c. Commission, pt 91

للأشخاص الذين شاركوا في اجتماع عمل والتي تظهر في محضر الاجتماع تعتبر أيضًا بيانات شخصية"[١].

كذلك فإن **المعلومات المتعلقة بوصفات الدواء** سواء كانت في شكل وصفات طبية فردية أو في شكل اتجاهات تم تحديدها من عدد معين من الوصفات الطبية، يمكن اعتبارها بيانات شخصية تخص الطبيب الذي وصف هذا الدواء، حتى لو بقي المريض مجهول الهوية ، وبالتالي، فإن توفير المعلومات المتعلقة بهذه الوصفات المكتوبة من قبل أطباء محددين أو يمكن التعرف عليهم لمصنعي المنتجات الطبية الخاضعة للوصفات الطبية يشكل نقلًا للبيانات الشخصية[٢].

بخصوص الفقه فإنه يعتبر أن **قائمة البيانات الشخصية طويلة ومتنوعة بشكل خاص :** قد تكون هذه البيانات موجودة في دليل العناوين المهنية ، أو غير المهنية، في قائمة العملاء، رقم لوحة السيارة، البيانات الببليوغرافية، تحديد الأطراف والقضاة والمتقاضين في قرارات المحكمة، النتائج الأكاديمية للطالب، الحساب البنكي الرقم والسجل وما إلى ذلك[٣].

[1] - CJUE (GC), 29 juin 2010, affaire n° C-28/08, Commission c. The Bavarian Lager Co. Ltd, pt 86
[2] - Groupe 29, Avis 4/2007 op cit, p. 7
[3]- Sarah Sadik op cit.p.21.

يتضمن مفهوم البيانات الشخصية كلاً من المعلومات الموضوعية (مثل صفة الدم بالنسبة للشخص المعنى[١]) ، والمعلومات القابلة للتحقق ، والمعلومات المتنازع عليها ، والمعلومات الذاتية، فتندرج آراء وتقييمات الأشخاص أيضًا ضمن مفهوم البيانات الشخصية[٢]، والتى تؤخذ ذلك في الاعتبار بشكل خاص عندما يرغب، على سبيل المثال، موظف ، أو مرشح للوظيفة ، أو طالب في ممارسة حقه في الوصول فيما يتعلق بتقييمه من قبل صاحب العمل (المستقبلي) ، أو نتائج امتحاناته[٣]، و يمثل هذا النوع الأخير من المعلومات جزءًا كبيرًا من معالجة البيانات الشخصية في قطاعات مثل الخدمات المصرفية، لتقييم موثوقية المقترضين[٤].

أما بخصوص **البيانات المادية التي تتعلق بالأشياء** فإن الفقه قد اعتبر أن هذه البيانات تعد بيانات شخصية إذا أمكن ربطها بأفراد معينين ومحددين[٥].

عادة ما تكون هذه الأشياء المادية مملوكة لشخص ما، أو قد تكون تحت تأثير خاص من الأشخاص ، أو يكون لها تأثير خاص على الأشخاص ، أو تكون بطريقة ما

[1] - Groupe 29, Avis 4/2007 op cit , p. 7
[2] - Ibid - CJUE, 20 décembre 2017, affaire n° C-434/16, Novak, pt 34.- B3 p.16
[3] - Cécile de Terwangne et al, op cit.p.16 - Sarah Sadik op cit.p.21.
[4] - Groupe 29, Avis 4/2007 op cit , p. 7
[5] - Cécile de Terwangne et al. op cit.p.16 - Sarah Sadik op cit.p.21

على مقربة مادية أو جغرافية من أشخاص أو أشياء أخرى ؛ لذلك يمكننا أن نعتبر أن هذه المعلومات تتعلق بهؤلاء الأشخاص بشكل غير مباشر فقط[١].

هذا يعنى إنشاء صلة بين البيانات والشخص الطبيعي ، حيث يجب أن "تهم" البيانات الشخص المعني، وفيما يتعلق بهذا الشرط الأخير، يتم الاكتفاء عندما تكون المعلومات مرتبطة بشخص معين، بسبب محتواها ، أو غرضها ، أو تأثيرها[٢].

ومن أمثلة تلك البيانات المادية التي والتي يمكن ربطها بأفراد محددين بيانات تعريف السيارة[٣] ، وصور الأقمار الصناعية[٤] ، والبيانات المساحية[٥] وبالتالي فإن قيمة المنزل

[1] - Groupe 29, Avis 4/2007 op cit, p. 10.

[2] -Cécile de Terwangne et al., op cit.p.16 - Degrave, É. (2018). Copies d'examen et protection des données à caractère personnel, observations sous C.J.U.E. (2e ch.), 20 décembre 2017. *Journal des Tribunaux*, (6734), 480-484.

[3]- Sarah Sadik op cit.p.21

[4]-Cécile de Terwangne et al. op cit.p.16 - Commission de la protection de la Vie privée (CPVP), avis 26/2006 du 12 juillet 2006 concernant l'utilisation d'images satellites afin de dépister et de constater des infractions aux normes urbanistiques

[5] - Cécile de Terwangne et al., op cit.p.16 - Sarah Sadik op cit.p.21- Comité sectoriel pour l'Autorité fédérale, délibération AF n° 02/2012 du 9 février 2012 concernant la demande du SPF Intérieur, Direction générale Sécurité civile, d'accéder à certaines données cadastrales (Documentation patrimoniale – SPF Finances) dans le cadre de la réforme des services de secours.

المرتبط بأصول مالكه[١]، أو بيانات الموقع الجغرافي لسيارات الأجرة المرتبطة بسائقيها تندرج ضمن فئة البيانات الشخصية[٢].

ينطبق هذا المبدأ أيضًا على البيانات المتعلقة في المقام الأول بالعمليات أو الأحداث، على سبيل المثال المعلومات المتعلقة بتشغيل آلة تتطلب تدخلًا بشريًا؛ لذلك من الممكن اعتبار هذا النوع من المعلومات "تخص" شخصًا طبيعيًا[٣].

فيما يتعلق بالحماية القانونية المرتبطة بالبيانات الشخصية ، فلا يهم شكل البيانات إذا تمت تغطية جميع أنواع المعلومات. فجميع الأشكال التي يمكن أن تتخذها المعلومات تقع ضمن مفهوم البيانات الشخصية إذا تم تغطية جميع العناصر التي تجعل من الممكن تحديد هوية الشخص الطبيعي[٤].

---

[١] – تشكل قيمة المنزل جزءًا من المعلومات حول كائن ما. من الواضح أن قواعد حماية البيانات لا تنطبق إذا تم استخدام هذه المعلومة فقط لتوضيح مستوى أسعار المنازل في منطقة معينة. ومع ذلك، في ظروف معينة، تستحق هذه المعلومات أيضًا اعتبارها بيانات شخصية. في الواقع، يشكل المنزل أصول المالك، والتي سيتم استخدامها، على سبيل المثال، لتحديد ما إذا كان هذا الشخص خاضعًا للضريبة بهذه الصفة. وفي هذا السياق، لا جدال في أن هذه المعلومات يجب أن تندرج ضمن فئة البيانات الشخصية.

Groupe 29, Avis 4/2007 op cit, p. 10.

[2] - Sarah Sadik op cit.p.21

[3] - Groupe 29, Avis 4/2007 op cit, p. 10.

[4] - Sarah Sadik op cit.p.22 - Cécile de Terwangne et al, op cit.p.16

فيما يتعلق بشكل المعلومات ، أو الوسيلة المستخدمة لها، فإن مفهوم البيانات الشخصية يشمل المعلومات المتاحة بأي شكل من الأشكال[١]:

يمكن أن تتخذ البيانات الشخصية شكل نص مكتوب سواء كان نصًا مكتوبًا بحروف أبجدية ، أو رقمية[٢]، أو رسمًا بيانيًا[٣]، أو صور فوتوغرافية ، أو أفلام فيديو[٤]، أو صوتًا(عينات صوتية) [٥].

[1] - Article 2 de la loi informatique et libertés et article 4 du RGPD.- Groupe 29, Avis 4/2007 op cit, p. 8

[2] Groupe 29, Avis 4/2007 op cit, p. 8

[٣] – "بعد اختبار نفسي عصبي تم إجراؤه على طفلة صغيرة في سياق الإجراءات القانونية المتعلقة بحضانتها، قامت برسم رسم يمثل عائلتها. يقدم هذا الرسم معلومات عن الحالة النفسية للفتاة ومشاعرها تجاه أفراد أسرتها المختلفين. ويمكن اعتبار هذه المعلومات في حد ذاتها "معلومات شخصية". وهذا الرسم يكشف في الواقع معلومات تخص هذا الطفل (صحته النفسية)، ولكن أيضاً سلوك والده أو والدته على سبيل المثال. وبالتالي، يمكن للوالدين في هذه الحالة استخدام حقهم في الوصول إلى هذه المعلومة المحددة.

Groupe 29, Avis 4/2007 op cit, p.9

[4] - Cécile de Terwangne et al. op cit.p.16.

بالنسبة للعديد من الحالات التي تعتبر فيها صور الأفراد في شكل صور فوتوغرافية ، أو أفلام فيديو بيانات شخصية.

Corr. Bruxelles (51e ch.), 14 janvier 2002, A.M, 2002, pp. 198 et s. ; Gand, 28 mars 2002, T. Strafr., 2002, liv. 6, p. 329 ; Liège (6e ch.), 27 juin 2003, R.D.T.I., 2004, n° 18, pp. 105 et s. ; Mons (1re ch.), 2 mai 2005, J.L.M.B., 2005, p. 1057

[٥]– " فيما يتعلق بالخدمات المصرفية الهاتفية، حيث يتم تسجيل صوت العميل الذي يعطي تعليمات للبنك، فإن هذه التعليمات المسجلة تعتبر بيانات شخصية"

Groupe 29, Avis 4/2007 op cit, p. 9

بخصوص البيانات التي تتكون من أصوات وصور فيبدو أنها تستحق، في حد ذاتها، الاعتراف بها كبيانات شخصية، بقدر ما يمكن أن تمثل معلومات عن شخص طبيعي[١].

علاوة على ذلك، لكي تعتبر هذه المعلومات بيانات شخصية، ليس من الضروري أن يتم تضمينها في قاعدة بيانات ، أو في ملف منظم. فيمكن التعرف على المعلومات الواردة في شكل نص حر في مستند إلكتروني على أنها بيانات شخصية، بشرط استيفاء المعايير الأخرى المنصوص عليها في تعريف البيانات الشخصية. على سبيل المثال تحتوي رسائل البريد الإلكتروني على "بيانات شخصية"[٢].

تتضمن البيانات الشخصية أيضًا فئات خاصة من البيانات، تسمى **بالبيانات "الحساسة"**، وهي البيانات "التي تكشف عن الأصل العنصري ، أو الاثني ، أو الآراء السياسية ، أو المعتقدات الدينية ، أو الفلسفية ، أو العضوية النقابية لشخص طبيعي، والبيانات الجينية، والبيانات البيومترية ، والبيانات المتعلقة بالصحة ، أو البيانات المتعلقة بالحياة الجنسية ، أو التوجه الجنسي لشخص طبيعي[٣].

تتوافق البيانات الحساسة مع فئات محددة من البيانات الشخصية التي يُحظر معالجتها– الحظر عام تمليه حقيقة أن البيانات المعنية من المحتمل في حد ذاتها أن

[1] - Groupe 29, Avis 4/2007 op cit, p. 9
[2] - Groupe 29, Avis 4/2007 op cit, p.8
[٣] - المادة الأولى من القانون رقم ١٥١ لسنة ٢٠٢٠- GDPR Art. 9 al.1

تنتهك الحريات الأساسية ، أو الحياة الخاصة– مع بعض الاستثناءات التي منها الموافقة الصريحة للشخص على معالجة هذه البيانات لغرض واحد أو أكثر ، وعلى أن تكون المعالجة ضرورية لحماية المصالح الحيوية للشخص المعنى ، باستثناء حالة الاتحاد الأوربي ، أو الدولة العضو التي ينص القانون على أن الحظر المشار إليه في الفقرة الأولى لا يمكن رفعه من قبل صاحب البيانات.

تقدم اللائحة العامة لحماية البيانات (RGPD) ، بالمقارنة مع التوجيه ٩٥/٤٦، فئتين جديدتين من البيانات الحساسة هما البيانات البيومترية والبيانات الجينية.

تعد **البيانات البيومترية** جزءًا من فئة البيانات الحساسة ويتم تعريفها قانونًا على أنها بيانات "ناتجة عن معالجة تقنية محددة، تتعلق بالخصائص الجسدية ، أو الفسيولوجية أو السلوكية للشخص الطبيعي، والتي تسمح أو تؤكد تحديد هويته بشكل فريد، مثل ملامح الوجه". الصور أو بيانات بصمات الأصابع[1].

تشمل الأمثلة النموذجية لهذه البيانات البيومترية بصمات الأصابع، وبنية الشبكية، وبنية الوجه، والصوت، و أيضًا شكل اليد، والجهاز الوريدي، وكذلك الخصائص السلوكية العميقة مثل التوقيع المكتوب بخط اليد، وديناميكيات الكتابة على لوحة المفاتيح، أو كلام معين، وما إلى ذلك.

[1] - GDPR Art. 4 al.14

١١ - حماية البيانات الشخصية عبر تقنية البلوك تشين

تتميز البيانات البيومترية، من بين أمور أخرى، بأنه يمكن اعتبارها محتوى معلومات تتعلق بشخص طبيعي معين (يمتلك X بصمات الأصابع هذه) ، بالإضافة إلى كونها عنصرًا يجعل من الممكن إنشاء صلة بين المعلومات والشخص الطبيعي[١].

يمكن أن تكون البيانات الشخصية الحساسة بيانات وراثية ، أو جينية ، وهى البيانات الشخصية المتعلقة بالخصائص الجينية الوراثية ، أو المكتسبة لشخص طبيعي ، والتي توفر معلومات فريدة عن علم وظائف الأعضاء ، أو الحالة الصحية لذلك الشخص الطبيعي والتي تنتج ، على وجه الخصوص، من تحليل عينة بيولوجية من الشخص الطبيعي المعني[٢].

وقد اعتبرت الهيئة الوطنية لتكنولوجيا المعلومات والحريات(CNIL) هذه البيانات مميزة ، حيث اعتبرتها مغايرة لكل البيانات الشخصية الأخرى ؛ وذلك لأنها تتمتع بالحميمة بشكل خاص ، مما يجعلها تحتاج لوضع قانوني وقائي للغاية[٣].

في الحقيقة إن البيانات الجينية تشكل حالة خاصة ، وهذه الخصوصية ليست كونها شخصية فحسب، بل أيضًا متعددة الأشخاص ؛ لأنها قابلة للانتقال والمشاركة.

---

[1] - Groupe 29, Avis 4/2007 op cit, p. 9
[2] - GDPR Art. 4 al.13
[3] - CNIL, Les Données génétiques, Point CNIL, 2017

ترتبط البيانات الجينية بالحمض النووي لحامله وتجعل من الممكن تمييزه عن جميع البشر الآخرين، ولكن هذه الجينات أيضًا مشتركة جزئيًا بين العديد من الأشخاص ، حيث يتم بناء الحمض النووي للفرد من الحمض النووي لوالديه ، لذلك كلما اقتربنا من شجرة عائلة الشخص، كلما كان حمضنا النووي أقرب.

لقد أصبح استغلال هذه البيانات، الذي اقتصر في البداية على المجال الطبي وتحديد الهوية القانونية، يميل إلى التطور في مجالات متنوعة بشكل متزايد: مثل التأمين، وعلم الأنساب، والتسويق، ومكافحة الهجرة، وما إلى ذلك.

في الحقيقة لم تكن القضايا الأخلاقية المتعلقة بالبيانات الجينية بمثل هذه الأهمية كما هي اليوم ، حيث مخاطر التلاعب الجيني ، والتمييز، والسيطرة على التراث الجيني للفرد، وتسليع البيانات، وما إلى ذلك [١].

كذلك من ضمن هذه الفئة من البيانات الحساسة، توجد **البيانات الصحية** التي يتم تعريفها في اللائحة العامة للبيانات (RGPD) على أنها "البيانات الشخصية المتعلقة

[1] - Jean-Marc ,Van GYSEGHEM et Cécile de Terwangne : « Analyse détaillée de la loi de protection des données et de son arrêté royal d’exécution », Vie privée et données à caractère personnel, Bruxelles, Politeia, 2013 p.259.

بالصحة الجسدية أو العقلية للشخص الطبيعي، بما في ذلك تقديم خدمات الرعاية الصحية، والتي تكشف عن معلومات حول الحالة الصحية لهذا الشخص[١]."

يعد هذا التعريف أوسع مما ظهر في التوجيه ٩٥/٤٦ ؛ لأنه لم يعد يغطي البيانات المتعلقة بالصحة وفقط، ولكنه يكشف معلومات عن الحالة الصحية ، وهذا يعني أنه بمجرد أن تكشف البيانات عن حالة الصحة بأصغر طريقة ممكنة، فهي بيانات خاصة بالمعنى المقصود في اللائحة العامة لحماية البيانات.

تعتبر البيانات الشخصية بيانات حساسة عندما يكون لها ارتباط واضح ووثيق بوصف الحالة الصحية للشخص: البيانات المتعلقة باستهلاك الأدوية ، أو الكحول ، أو المخدرات والبيانات الوراثية هي بلا شك "بيانات شخصية تتعلق بالصحة"، ولا سيما إذا تم تسجيلها في ملف طبي.

بالإضافة إلى ذلك، فإن أي بيانات أخرى – على سبيل المثال البيانات الإدارية (رقم الضمان الاجتماعي، تاريخ الدخول إلى المستشفى، وما إلى ذلك) – تكون واردة في الوثائق الطبية المتعلقة بعلاج المريض يجب أن تعتبر حساسة ؛ لأنها إذا لم تكن

[1] - GDPR Art. 4 al.15

ذات صلة بحالة المريض وعلاجه لم يكن من الممكن، ولا ينبغي أن يتم إدراجها في السجل الطبي"[١].

إن البيانات الشخصية تتوافق مع أي معلومات تتعلق بشخص طبيعي ، أو تسمح بالتعرف عليه.

يتناول مصطلح الشخص الطبيعي **الأفراد الأحياء** ، وهذا يعنى أنه من حيث المبدأ فإن المعلومات المتعلقة بالأفراد المتوفين لا تعتبر بيانات شخصية ، ولا تخضع لقواعد الحماية؛ حيث أن الموتى لم يعودوا أشخاصًا طبيعيين في القانون المدني[٢] ، كذلك الحال بخصوص بيانات الأشخاص الاعتبارية الخاصة.

بخصوص بيانات **الأشخاص المتوفين** فإنها رغما عن ذلك قد تظل في بعض الحالات تستفيد بشكل غير مباشر من مستوى معين من الحماية.

من ناحية ، قد لا يتمكن مراقبو البيانات من التحقق مما إذا كان الشخص الذي تتعلق به البيانات لا يزال على قيد الحياة أو ربما ميتًا.

من ناحية أخرى ، يمكن اعتبار المعلومات التي تمثل بيانات تتعلق بالأشخاص المتوفين تتعلق بأشخاص أحياء في نفس الوقت وتشكل بيانات شخصية– موضوع

[1] - Jean-Marc et al., op. cit. p.264.
[2] - Supriya Adhatarao. op. cit. p.14.

البيانات ذات الصلة، مثل أحد أفراد الأسرة ، وفى هذه الحالة فإن البيانات الشخصية للأشخاص المتوفين قد تستفيد بشكل غير مباشر من حماية قواعد حماية البيانات[1].

كذلك فإن المعلومات المتعلقة بالأشخاص المتوفين قد تستفيد من الحماية المحددة التي تمنحها سلسلة من القواعد غير تشريعات حماية البيانات، كالتزام العاملين في المجال الطبي بالسرية والتي لا تنتهي بوفاة المريض، وكذلك التشريعات المتعلقة بالحق في احترام الصورة ، والشرف ، وحماية ذكرى الشخص المتوفى.

أما بخصوص تطبيق قواعد حماية البيانات على **الطفل الذى لم يولد بعد**(الجنين) فتعتمد إمكانية تطبيق قواعد حماية بيانات ما قبل الولادة على النهج العام المعتمد في الأنظمة القانونية الوطنية فيما يتعلق بحماية الأطفال الذين لم يولدوا بعد.

تعترف بعض الدول الأعضاء بالاتحاد الأوربي ، لمراعاة حقوق الميراث بشكل أساسي، بالمبدأ الذي بموجبه يعتبر الأطفال الذين في فترة الحمل (أجنة) ولكن لم يولدوا بعد ، كما لو كانوا قد ولدوا فيما يتعلق بحقوق معينة كالميراث ، وقبول التبرع ، بشرط أن يولدوا بالفعل.

من أجل تحديد ما إذا كانت أحكام حماية البيانات الوطنية تحمي أيضًا المعلومات المتعلقة بالأطفال الذين لم يولدوا بعد، فمن المناسب النظر في النهج العام للنظام

[1]- Groupe 29, Avis 4/2007 op cit, p. 25 - Mirko Koscina op.cit.p.16.

القانوني الوطني، مع الأخذ في الاعتبار أن الغرض من قواعد حماية البيانات هو حماية الشخص الطبيعي.

في الواقع يجب ألا تقتصر الحماية إلى المعلومات المتعلقة ببيانات الأطفال الذين لم يولدوا بعد على مدة الحمل ، وإنما يجب أن يؤخذ بعين الاعتبار مد الحماية للأجنة المجمدة ، خاصة المعلومات الطبية ، والوراثية عن هذه الأجنة[١].

أما بخصوص **بيانات الأشخاص الاعتبارية الخاصة** فهي تعد جزءًا من فئة واسعة من البيانات غير الشخصية التي تشمل جميع البيانات التي لا تحدد هوية الشخص الطبيعي ، أو لا تسمح بتحديد هويته ، وبالتالي لا تغطيها اللائحة العامة للبيانات من حيث المبدأ، وبالتالي لا تستفيد من الحماية التي توفرها[٢].

مع ذلك، قد تظل بعض قواعد حماية البيانات تنطبق بشكل غير مباشر على المعلومات المتعلقة بالشركات ، أو الكيانات القانونية، في ظروف معينة[٣].

يمكن اعتبار المعلومات المتعلقة بالأشخاص الاعتباريين "تخص" الأشخاص الطبيعيين بهذه الصفة عندما يكون اسم الكيان القانوني مشتقًا من اسم شخص طبيعي، أو السيناريو الآخر هو البريد الإلكتروني الخاص بالشركة والذي يستخدمه

[1] - Groupe 29, Avis 4/2007 op cit, p. 25-26
[2] - Sarah Sadik, op.cit.p.23-24.
[3] - Groupe 29, Avis 4/2007 op. cit p. 26

الموظف عادةً ، أو معلومات حول شركة صغيرة والتي من المحتمل أن تصف سلوك مالكها .

في جميع هذه الحالات، عندما تتيح معايير المحتوى ، أو الغرض ، أو النتيجة اعتبار المعلومات المتعلقة بشخص اعتباري ، أو شركة تخص شخصًا طبيعيا، فمن المناسب اعتبارها بيانات شخصية ، وبالتالي يجب تطبيق قواعد حماية البيانات الشخصية[١].

بخصوص الشخص الطبيعي ، بشكل عام، يمكن اعتباره "محدد الهوية" عندما "يميز" نفسه ضمن مجموعة من الأشخاص عن جميع الأعضاء الآخرين في تلك المجموعة.[٢].

بموجب اللائحة العامة لحماية البيانات، فإن أي معلومات تتعلق بشخص طبيعي- محدد أو يمكن تحديد هويته- تشمل حاليًا كلاً من المعرفات المباشرة وغير المباشرة.

تشير اللائحة العامة لحماية البيانات إلى هذه "المعرفات" في تعريف "البيانات الشخصية" ، والتي تنص على أنه "يجوز تحديد هوية الشخص الطبيعي، بشكل مباشر أو غير مباشر، ولا سيما بالإشارة إلى رقم تعريف ، أو إلى واحد ، أو أكثر

[1] - Groupe 29, Avis 4/2007 op cit, p. 26
[2] - Groupe 29, Avis 4/2007 op. cit p. 12

عناصر محددة خاصة بهوية الفرد الجسدية ، أو الفسيولوجية ، أو النفسية ، أو الاقتصادية ، أو الثقافية ، أو الاجتماعية[1].

يمكن تعريف أدوات التعريف المباشرة بأنها تلك المعلومات التي تحدد هوية الشخص بشكل صريح (مثل الاسم ، أو رقم الضمان الاجتماعي ، أو البيانات البيومترية).

أما **المعرفات غير المباشرة** ، أو شبه المباشرة فإنها تشير إلى المعلومات التي يمكن دمجها مع بعض البيانات الإضافية لتحديد هوية شخص معين (مثل مزيج الجنس ، أو تاريخ الميلاد ، أو المؤشر الجغرافي ، أو السجلات الطبية ، أو المعلومات المالية وما إلى ذلك).

بخصوص **الاسم كأحد المعرفات المباشرة** ، فمن المعتاد أن يكون للأفراد اسم شخصي يتم استخدامه بشكل أساسي لتحديد هوية الفرد، ويمكن أن يكون كلمة أو مجموعة من الكلمات التي يتم من خلالها معرفة الشخص ، أو الشيء ، أو مخاطبته ، أو الإشارة إليه.

في الواقع طالما كانت هناك لغات، كانت هناك أسماء. فالتسمية تميز شخصًا واحدًا عن الآخرين ، وفي الغالب كل مجتمع لديه نظام تسمية خاص به ، وتقع الأسماء

[1] - GDPR Art. 4.

وبخاصة أسماء العائلات في قلب تاريخ كل أمة : وهي مثال رئيسي للعقد الاجتماعي الذي يربط الناس معًا في المجتمع.

بخصوص نظام التسمية الفرنسي عادة ما يتم اختيار الأسماء الأولى في فرنسا من قبل والدي الطفل.

في الوقت الحاضر لا توجد قيود قانونية مسبقة على اختيار الاسم الأول، ولكن في القرن الثامن عشر، كان اختيار الأسماء المحددة مقيدًا في الأصل بموجب القانون فقط بتقليد تسمية الأطفال بأسماء عدد صغير من القديسين المشهورين ، وفي وقت لاحق من عام ١٩٦٦، سمح قانون جديد بعدد محدود من الأسماء الأسطورية ، أو الإقليمية ، أو الأجنبية ، وأخيراً في عام ١٩٩٣، مُنح الآباء الفرنسيون حرية تسمية أطفالهم دون أي قيود[1].

في العصور الوسطى ، كان من الضروري إضافة اسم العائلة للتمييز بين الأفراد الذين يحملون نفس الاسم الأول.

في البداية، كان من السهل اعتماد أي اسم عائلة يرغب فيه الناس حتى عام ١٤٧٤ ثم أصدر ملك تلك الفترة مرسومًا يقضي بأن جميع تغييرات الاسم الأخير يجب أن

[1] - Supriya Adhatarao op. cit. p.15. - Powell, Kimberly. "French Surname Meanings and Origins." ThoughtCo, Aug. 29, 2020, thoughtco.com/french-surname-meanings-and-origins-1420788

تمر بموافقته. ومنذ ذلك الحين، تم تسجيل جميع تغييرات الأسماء مما ساعد أيضًا في تسهيل تتبع تاريخ العائلة[١].

تجميع الأسماء الأخيرة الفرنسية في أنواع مختلفة: منها الألقاب العائلية حيث كان استخدام أسماء الوالدين الطريقة الشائعة جدًا لبناء الألقاب والتي كانت تعتمد عادةً على اسم الأب ، كما كانت تستند إلى اسم الأم عندما كان اسم الأب غير معروف.

كما كان هناك أيضا الألقاب المهنية، حيث كان من الشائع أيضًا التمييز بين الأفراد من خلال الإشارة إلى وظائفهم ، أو مهنهم مثل Caron (صانع العجلات) ، Berger (الراعي)، Charpentier (النجار).

كذلك وجدت الألقاب الوصفية، حيث تم إنشاء بعض الألقاب بناءً على مظهر الأفراد، وصفاتهم الفريدة، وأيضًا من ألقابهم ، أو أسماء حيواناتهم الأليفة ، من بعض الأمثلة الشائعة تشمل Jacques Legrand بالنسبة لجاك الكبير ، (Petit) الصغير، Brun (شخص ذو شعر بني أو بشرة بنية) LeBlanc (شعر أشقر أو بشرة فاتحة) وما إلى ذلك.

في فرنسا يحتفظ المعهد الوطني للإحصاء والدراسات الاقتصادية (INSEE) بسجلات لجميع الأسماء الأولى والأخيرة للمواطنين الفرنسيين[١].

[1] - Powell, Kimberly. Op .cit

١١ - حماية البيانات الشخصية عبر تقنية البلوك تشين

إن جميع البلدان الأخرى في جميع أنحاء العالم ، تعتبر مثل فرنسا، لديها نظامها الخاص لتسمية الأفراد. حيث تحددنا أسماؤنا كأفراد ، وأيضًا كأعضاء في مجموعة ، أو مجتمع معين[٢].

قد يظن المرء أن اسم شخص ما هو مثال واضح للبيانات الشخصية، فهو حرفيًا ما يميز الشخص. لكن الأمر ليس بهذه البساطة دائمًا.

عادةً ما يتم استخدام الاسم الكامل للشخص لتحديد هويته للأغراض القانونية والإدارية ، مع ذلك فإننا نرى أنه في بعض الأحيان قد لا يكون الاسم الكامل الذي يُعرف به الفرد بشكل عام ؛ ذلك أن البعض يستخدم جزءًا فقط من أسمائهم الكاملة ، أو يُعرف البعض الآخر بألقابهم ، أو الأحرف الأولى من أسمائهم ، أو بأسماء مستعارة ، أو غيرها من التسميات الرسمية ، أو غير الرسمية[٣].

---

[١] - يقوم المعهد الوطني للإحصاء والدراسات الاقتصادية بجمع وإنتاج وتحليل ونشر المعلومات عن الاقتصاد والمجتمع الفرنسي ، وقد تم إنشاؤه بموجب قانون الميزانية في ٢٧ أبريل ١٩٤٦.
في كل عام، يقوم المعهد الوطني للإحصاء والإحصاءات (INSEE) بتقدير عدد سكان المناطق والمقاطعات (فرنسا الكبرى وDOM) اعتبارًا من الأول من يناير. يتم تقسيم هذه التقديرات السكانية السنوية حسب الجنس والعمر وغيرها من المعلومات.
INSEE) Institut national de la statistique et des études économiques
https://www.insee.fr/fr/accueil.

[2] - Supriya Adhatarao op. cit. p.16.

[3] - Powell, Kimberly. Op.cit

فيما يتعلق بالأشخاص الذين تم تحديد هويتهم ، أو الذين يمكن التعرف عليهم "بشكل مباشر"، من الواضح أن اسم الشخص هو المعرف الأكثر شيوعًا، وفي الممارسة العملية، غالبًا ما يشير مصطلح "الشخص المحدد" إلى إشارة إلى اسم ذلك الشخص[1]. عندما تكون الأسماء الأولى نادرة ، أو فريدة من نوعها، فباستخدام المعرفات غير المباشرة (معلومات عن الجنس ، وسنة الميلاد ، وعدد الأشخاص الذين يمتلكون الاسم في قسم معين) فمن الممكن تحديد شخص معين.

أما بخصوص **الأسماء الأخيرة الفريدة** ، باستخدام الإحصائيات المتاحة للأسماء الأخيرة في فرنسا، والتي تتضمن مجموعة بيانات بالاسم الأخير لجميع الأسماء الأخيرة المسجلة من عام ١٨٩١ إلى ٢٠٠٠.

باستخدام مجموعة البيانات هذه، نجد أن هناك عدد كبير من الأسماء الأخيرة التي تحظى بشعبية كبيرة، وبالتالي فإنها لا تشكل بيانات شخصية في جميع الأوقات.

في هذه الحالة، لتحديد هوية شخص معين، يتم استخدام شبه معرفات مثل الاسم الأول ، والقسم ، والجنس ، وتاريخ الميلاد ، وما إلى ذلك.

بخصوص الأسماء الأخيرة الفريدة التي يستخدمها شخص واحد فقط في فرنسا. فإنه يمكن التعرف على ما لا يقل عن ١٠٩٠ شخصًا فقط بناءً على اسم عائلتهم الفريد

[1]- Groupe 29, Avis 4/2007 op cit, p. 14.

في فرنسا ، وتعد هذه الأسماء الأخيرة الفريدة بيانات شخصية تؤدي إلى تحديد هوية الفرد فقط باستخدام اسمه الأخير في فرنسا.

لا شك أن الأسماء الفريدة تجعل تطبيق اللائحة العامة لحماية البيانات أسهل على مراقبي البيانات للتحقق من صاحب البيانات، لكنها تفرض مخاطر أعلى على الخصوصية، كما يسهل التعرف على هؤلاء الأفراد ، وهذا عكس الاسم الكامل للشخص الذى يعد المثال الأكثر وضوحًا للمعلومات الشخصية[١].

في الحقيقة فإن الاسم عبارة عن معلومة تكشف أن الشخص يستخدم هذا المزيج من الحروف والأصوات ليميز نفسه عن الآخرين ، وليتميز عن الأشخاص الذين يقيم معهم علاقات.

يمكن أن يكون الاسم أيضًا نقطة البداية المؤدية إلى معلومات حول منزل الشخص، أو مكان وجوده ، ومعلومات عن أفراد عائلته (من خلال اللقب) ، والعلاقات المختلفة ، والمسائل القانونية والاجتماعية المرتبطة بهذا الاسم (التعليم/الدراسات، السجلات الطبية، الحسابات المصرفية). بل إنه من الممكن معرفة مظهر الشخص إذا كانت صورته مرتبطة بهذا الاسم.

[1] - Supriya Adhatarao op. cit. p.20.

كل هذه العناصر الجديدة من المعلومات المرتبطة بالاسم يمكن أن تسمح لشخص ما "بتكبير" الشخص من لحم ودم، وبفضل المعرفات، يتم بعد ذلك ربط العنصر الأولي من المعلومات بشخص طبيعي "يمكننا تمييزه" عن أشخاص أخرين[١].

في الواقع، عادةً ما تقوم ملفات الكمبيوتر التي تسجل البيانات الشخصية بتعيين معرف محدد للأشخاص المسجلين لتجنب أي خلط بين شخصين موجودين في نفس الملف.

على الإنترنت أيضًا، تُسهل أدوات مراقبة حركة المرور فهم سلوك الآلة، ومن خلفها، سلوك مستخدمها، وبذلك نقوم بإعادة بناء شخصية الفرد لإسناد قرارات معينة إليه ومن دون حتى الاستفسار عن اسم الشخص وعنوانه، يمكن وصفهما وفقا لمعايير اجتماعية ، واقتصادية ، أو نفسية ، أو فلسفية ، أو غيرها، وأن ننسب قرارات معينة إليهما ، وبعبارة أخرى، فإن إمكانية التعرف على شخص ما لم تعد تعني بالضرورة القدرة على معرفة هويته ، وهذه الملاحظة نجدها في تعريف مفهوم البيانات الشخصية[٢].

[1] - Groupe 29, Avis 4/2007 op cit, p. 14

[2] - Poullet Y. et son équipe, «Rapport sur l'application des principes de protection des données aux réseaux mondiaux de télécommunications», Conseil de l'Europe, Comité consultatif T-PD, point 2.3.1, T-PD (2004) 04 final

وقد قضت محكمة العدل التابعة للجماعات الأوروبية في هذا الشأن بأن "العملية التي تتمثل في الإشارة، على صفحة إنترنت إلى أشخاص مختلفين والتعرف عليهم إما بأسمائهم ، أو بوسائل أخرى، على سبيل المثال رقم هاتفهم ، أو المعلومات المتعلقة بظروف عملهم ، وهواياتهم، تشكل "معالجة البيانات الشخصية"[1].

بخصوص **الاسم المستعار** فإنه يتكون من إخفاء الهوية ، ويعد أحد مستجدات اللائحة العامة لحماية البيانات مقارنة بتوجيه حماية البيانات لعام ١٩٩٥.

تقدم المادة ٤ فقره ٥ من القانون العام لحماية البيانات الاسم المستعار باعتباره معالجة للبيانات الشخصية بطريقة لا يمكن من خلالها نسب البيانات الشخصية إلى صاحب بيانات محدد دون استخدام معلومات إضافية، بشرط أن يتم الاحتفاظ بهذه المعلومات الإضافية بشكل منفصل وتخضع لإجراءات فنية وتنظيمية. للتأكد من أن البيانات الشخصية لا تنسب إلى شخص طبيعي محدد ، أو يمكن تحديد هويته.

لم يتم وصف طرق محددة ، بما يتماشى مع روح اللائحة المحايدة من الناحية التكنولوجية. وهذا يؤكد أن البيانات ذات الأسماء المستعارة تظل بيانات شخصية،

[1] - Arrêt du 6 novembre 2003 dans l'affaire C-101/2001 (Lindqvist), point 27.

وذلك تماشيًا مع النتيجة التي توصلت إليها فرقة العمل المعنية بالمادة ٢٩ بأن "الأسماء المستعارة ليست وسيلة لإخفاء الهوية"[1].

أما بخصوص **عناوين IP الديناميكية** وهل هي بيانات شخصية أم لا ؟ للإجابة على هذه التساؤل يجب أن نعرف أولا مفهوم عناوين IP الديناميكية.

يعتبر الإنترنت شبكة ضخمة من مليارات الأجهزة المتصلة التي تتواصل مع بعضها البعض بشكل يومي لإرسال واستقبال البيانات. تتصل أجهزة الكمبيوتر والأجهزة الأخرى بالشبكة باستخدام اتصالات سلكية ، أو لاسلكية.

تعد عناوين IP العمود الفقري للإنترنت ؛ حيث يتم استخدامها لتحديد الأجهزة ، وتقوم كل خوادم الويب تقريبًا بمعالجتها في سجلها.

عنوان IP (عنوان بروتوكول الإنترنت) هو رقم تعريف لجهاز الشبكة المتصل بالإنترنت، وهو عنوان رقمي للجهاز؛ نظرًا لأن الأجهزة الموجودة على الإنترنت تتبادل البيانات، فإنها تحتاج إلى هوية رقمية للتواصل. وبالتالي، يتضمن كل جهاز متصل عنوانًا رقميًا يعرف باسم عنوان IP.

يحتوي الكمبيوتر المحمول ، والهاتف الذكي ، والأضواء الذكية ، وأجهزة مراقبة الأطفال ، والأجهزة اللوحية ، ومنظم الحرارة ، والعديد من الأجهزة الأخرى المتصلة

[1] - Groupe 29, Avis 4/2007 op cit, p. 19.

بالإنترنت على عنوان IP. على هذا النحو، في كثير من الحالات، من الممكن افتراض وجود اتصال قوي بين الجهاز ومستخدمه[١].

الواقع أن السوابق القضائية الفرنسية ، وكذلك الأوروبية أيضا تميل في السنوات الأخيرة إلى توسيع مفهوم البيانات الشخصية، وبالتالي توسيع نطاق تطبيق القواعد في هذا المجال.

وقد تم تأكيد هذا الاتجاه بشكل ملحوظ من خلال القرارات الأخيرة لكل من محكمة العدل التابعة للاتحاد الأوروبي (CJEU)[٢]التي احتفظت بتصنيف عناوين IP الديناميكية كبيانات شخصية.

قامت محكمة العدل الأوربية بدراسة متأنية لاستخدام مصطلح " بشكل غير مباشر " الذى قدمه المشرع في المادة الثانية من القانون رقم ٧٨-١٧ المعلوماتية ، والحريات المتعلقة بتعريف مفهوم البيانات الشخصية ، والتي جاءت على النحو التالي "أي معلومات تتعلق بشخص طبيعي تم تحديد هويته ، أو يمكن التعرف عليه، بشكل مباشر ، أو غير مباشر، بالرجوع إلى رقم تعريفي أ، و إلى عنصر ، أو أكثر خاص به".

[1] - Supriya Adhatarao op cit p.34 - Pavol Sokol, Jakub Mísek, and Martin Husák. „Honeypots and honeynets: issues of privacy“. In:EURASIP Journal on Information Security2017 (2017) pp. 1–9

[2] - CJUE, 19 oct. 2016, aff. C-582/14, Patrick Beyer c/ Bundesrepublik Deutschland

قررت المحكمة أن كلمة "بشكل غير مباشر" الواردة بهذه المادة كلمة لها قيمتها ، وتميل إلى الإشارة إلى أنه من أجل تصنيف المعلومات كبيانات شخصية، ليس من الضروري أن تسمح هذه المعلومات، في حد ذاتها، بتحديد هوية الشخص المعني.

وقد ذكر المحامي العام في رأيه أمام محكمة العدل الأوربية أن "عنوان IP الذي يخزنه مزود الخدمة فيما يتعلق بالوصول إلى صفحة الويب الخاصة به يشكل بيانات شخصية لمزود الخدمة هذا، طالما أن مزود خدمة الإنترنت لديه بيانات إضافية متاحة تجعل من الممكن التعرف على موضوع البيانات"[١].

كما أن محكمة النقض الفرنسية تبعتها في ذات الاتجاه من خلال إلغاء قرار يقضي بأن عنوان IP يتكون فقط من أرقام تتعلق بجهاز كمبيوتر وليس بمستخدم ، واتبعت المحكمة نفس المنطق الذي اتبعته محكمة العدل الأوروبية من خلال التأكيد على أهمية مصطلح "بشكل غير مباشر" في تعريف قانون حماية البيانات[٢].

كذلك استهدفت اللائحة العامة لحماية البيانات (GDPR) في الحيثية الثلاثين عناوين IP التي "عند دمجها مع المعرفات الفريدة ، والمعلومات الأخرى التي تتلقاها الخوادم،

[1] - Pavol Sokol et Autres,op. cit p.6 - Advocate general: paragraph 78 of the opinion of advocate general Campos Sánchez-Bordona Delivered on 12 May 2016 on the case C582/14 Patrick Breyer V Bundesrepublik Deutschland. Luxembourg (2016). Advocate General

[2] - Cass. 1re civ., 3 nov. 2016, n° 15-22.595 et J. Hauser, L'adresse IP est un élément d'identification, RTD civ. 2017, p. 94

يمكن استخدامها لإنشاء ملفات تعريف للأشخاص الطبيعيين ، وتحديد هوية هؤلاء الأشخاص"[١].

كما اعتبرت مجموعة عمل المادة (٢٩) أنه ينبغي تصنيف عناوين IP على أنها بيانات شخصية ، حيث قررت أن عناوين IP بمثابة بيانات تتعلق بفرد يمكن تحديد هويته. كما حددت في وثيقة عمل أنه "يمكن لمقدمي خدمات الإنترنت ومديري الشبكات المحلية، باستخدام وسائل معقولة، تحديد مستخدمي الإنترنت الذين خصصوا لهم عناوين IP ؛ لأنهم يسجلون بشكل منهجي في ملف التاريخ ، والوقت ، والمدة ، وعنوان IP الديناميكي تعطى لمستخدم الإنترنت.

ينطبق الشيء نفسه على مزودي خدمة الإنترنت الذين يحتفظون بملف التسجيل على خادم HTTP. في هذه الحالات، يمكننا التحدث، دون أدنى شك، عن البيانات الشخصية بالمعنى المقصود[٢].

كما أن (CNIL) خلال مداولاتها، اعتبرت أن عنوان IP لمستخدمي الإنترنت "يشكل بيانات شخصية ؛لأنه يجعل من الممكن التعرف بشكل غير مباشر على الشخص الطبيعي الذي لديه اشتراك في الإنترنت"[١].

[1]- RGPD, consid. 30.
[2] - Groupe 29, Avis 4/2007 op cit, p. 18

كما أن بعض الفقه يرى أنه من الآمن اعتبار عناوين IP شخصية بغض النظر عن المعلومات الاضافية الأخرى التي يمتلكها المشغل من عدمه ؛ ويعلل رأيه بأن المبدأ الوقائي الأساسي لنظام حماية البيانات الشخصية، وهو الذي ينظم كمية البيانات المجمعة، بحيث لا يمكن ربطها وإساءة استخدامها، كما أنه على الرغم من أنه في عدد من الحالات لا يمكن توصيل عناوين IP إلا بجهاز وليس بإنسان (مثل إنترنت الأشياء)، إلا أنه لا توجد طريقة سهلة لتمييزها.

وهذا يعني أن عناوين IP لن تكون بيانات شخصية في حالة عدم وجود بيانات إضافية ؛ لأنه لن يمكن التعرف على الشخص الطبيعي بالوسائل المتاحة للمشغل، خاصة أنه في معظم الحالات، يتم تنفيذ الهجوم بواسطة آلة ، وليس بواسطة إنسان ، وفي هذه الحالة، يكون تحديد هوية الشخص الطبيعي أمرًا صعبًا إلى حد ما[٢].

[1] - Délib. 2006-294 du 21 déc. 2006
[2] - Pavol Sokol et Autres,op. cit p.6

المطلب الثاني

البيانات الشخصية لمستخدم البلوك تشين

اعتمادًا على البروتوكول الذي تستخدمه سلاسل الكتل، والذي يمكن أن يكون عامًا ، أو خاصًا[١]، ستختلف طبيعة البيانات التي يتم جمعها ومعالجتها، ومن المحتمل أن تحتوي سلاسل الكتل هذه على بيانات شخصية[٢].

مسألة ما إذا كانت البيانات التي تتم معالجتها على البلوك تشين شخصية ، أو بأسماء مستعارة ، أو على العكس من ذلك مجهولة تمامًا هي شرط أساسي ؛ لأنه يحدد تطبيق اللائحة العامة لحماية البيانات (RGPD) من عدمه[٣].

إن البيانات الشخصية التي تتم معالجتها على البلوك تشين تختلف وفقًا لمواصفاتها.

تحتوي المعاملات في البلوك تشين على نوعين من البيانات – ذات طبيعة شخصية عند الاقتضاء – **البيانات الوصفية**، من ناحية، مثل العنوان العام للمستفيد من المعاملة، ومن ناحية أخرى، **البيانات المتعلقة بمحتوى المعاملة** التي قد تظهر في

[١] - فيما يتعلق بالبلوك تشين الخاص ، فكثيرا ما تقوم سلاسل الكتل الخاصة أحيانًا بجمع البيانات الشخصية (البيانات المصرفية، والبيانات الصحية، وما إلى ذلك، أو بيانات متعلقة بالتأمين، أو حتى بالعقارات).
Florence Chafiol, La blockchain à l'heure de l'entrée en application du règlement général sur la protection des données, Dalloz IP/IT 2017 p.637

[2] - Ibid.

[3] - RGPD, art. 4 et consid. 26.

نص عادي، أو تكون مشفرة، أو مجزأة (تظهر بصمة البيانات فقط في السجل، ويتم الاحتفاظ بالبيانات العادية خارج البلوك تشين) ، أو روابط تشير إلى خوادم خارجية[1] .

في النماذج الأولى لسلسلة الكتل العامة تم تصميم عملة البيتكوين المشفرة منذ البداية ؛ لتوفير شكل من أشكال الأسماء المستعارة والتي أشار إليها مصممها ساتوشي ناكاموتو باسم "عدم الكشف عن الهوية".

استخدم البلوك تشين العام عدم الكشف عن الهوية من خلال تقنية التشفير غير المتماثل، وفقًا لهذه الطريقة، يحتفظ كل من المشاركين في المعاملة بمفتاحين يعملان كزوج: مفتاح عام يتوافق مع عنوان عام عشوائي يتكون من أرقام وحروف (معلومات عامة) ، ومفتاح خاص يتوافق مع كلمة المرور (معلومات خاصة).

يتم إنشاء **العنوان العام** بواسطة محفظة المستخدم ، دون أن يحتاج الأخير إلى الكشف عن هويته.

يمكن للمستخدمين إنشاء عدد من المحافظ للاحتفاظ بعملات البيتكوين، ولا توجد قيود على عدد المحافظ التي يمكنهم امتلاكها، ولا توجد أي متطلبات لفتح المحفظة.

كما يتم نقل العملات المعدنية من محفظة إلى أخرى، وتوفر العلاقة الغامضة بين المحافظ والأشخاص الحقيقيين درجة من الخصوصية[1] .

[1] - Thibault Douville op cit n° 14.

نظرًا لعدم الكشف عن هوية المستخدم وتوقيعه على المعاملة، فمن غير الممكن الربط بين الاثنين بشكل مباشر، حيث إنه بمجرد التحقق من صحتها بواسطة الشبكة، ستعرض المعاملة المرئية للجميع في السجل فقط بيانات المعاملة (العناوين العامة، والأصول الرقمية، ومعرف المعاملة).

في الأصل، لا يمكن تصنيف العناوين العامة الأولى التي يمكن الوصول إليها في السجل على أنها بيانات شخصية ؛ لأنها لم تكن محددة، مما أدى فعليًا إلى عدم قابلية تطبيق اللائحة العامة لحماية البيانات على نماذج البلوك تشين هذه[٢].

مع ذلك، فإن علاقة **الاسم المستعار** بين المستخدمين ، والمحافظ ليست إخفاءً كاملاً للهوية ؛ ذلك أن سلاسل المعاملات داخل وخارج المحافظ، ومن محفظة إلى محفظة، مرئية للجميع، ويمكن تتبعها بشكل عام[٣]، وسيكون من الممكن إعادة بناء تصرفات الشخص من خلال متابعة تاريخ المعاملات، ولا سيما خلال الاستخدامات المتعددة لنفس العنوان العام لتنفيذ معاملات مختلفة ، وفي هذه الحالة سيتم الكشف عن هوية الشخص[٤].

[1] - Uk Government Office for Science, Distributed Ledger Technology : beyond Block chain, 2016, p. 50.
[2] - Florence Chafiol. op cit p.4.
[3] -Uk Government Office for Science, Distributed Ledger Technology op cit p. 50
[4] - Florence Chafiol. op cit p.4

وقد كان هذا الشكل الضعيف من الأسماء المستعارة، إلى جانب شفافية المعاملات على سلسلة كتل البيتكوين، يمثل في الواقع تحديًا للخصوصية ، على عكس المدفوعات التقليدية عبر الإنترنت، والتي تكون مرئية فقط للأطراف المتعاملة والمؤسسات المالية.

في البيتكوين يتم تسجيل المدفوعات – بما في ذلك المحافظ المعنية، والوقت التقريبي للمعاملة، وقيم المعاملة – في سلسلة كتل مرئية للعامة ، والتي يمكن لأي شخص معالجتها ، واستخلاص استنتاجات حولها. فعلى سبيل المثال، حجم مبيعات التاجر عبر الإنترنت، أو الملف الشخصي للشراء لمستخدم معين، أو حتى التحويلات العديدة بين الأفراد[1].

بخصوص البيتكوين من الآن فصاعدا، يقوم المشاركون بشراء هذه العملات الافتراضية مباشرة على المنصات ، ويتم التعدين بواسطة خوادم – معظمها موجود في الخارج – بقدرات حسابية كبيرة للغاية. في هذا الصدد، قد تحتفظ بعض منصات تبادل العملات الافتراضية – مكاتب الصرافة "الإلكترونية" – مقابل العملات القانونية بالبيانات الشخصية للمستخدم.

[1] - Uk Government Office for Science, Distributed Ledger Tech n° logy op. cit p. 51

١١ - حماية البيانات الشخصية عبر تقنية البلوك تشين

تتمثل "الممارسات الجيدة" التي تنفذها معظم هذه المنصات في ضمان الهوية الحقيقية لعملائها من خلال مطالبتهم بتوصيل البيانات الشخصية مثل: الاسم، الاسم الأول، بيانات التحقق من كلمة المرور، تاريخ الميلاد، عنوان البريد الإلكتروني، رقم الهاتف، الوظيفة ، بطاقة الائتمان، بطاقة الهوية[١].

ولقد أصدرت هيئة الرقابة الاحترازية الفرنسية ، من جانبها، قرارًا في ٣٠ مارس ٢٠١٧ يقضي بمعاقبة شركة Lemon Way بتوبيخ وغرامة قدرها ٨٠,٠٠٠ يورو، على وجه الخصوص، لعدم تحديد العملاء الذين نفذوا عمليات شراء وبيع البيتكوين وفقا لنص المادة ٥/٥٦١ من القانون المالي[٢].

بخصوص **المفتاح العام** في البلوك تشين فإنه يعمل كنوع من المعرفات المذكورة سابقا. وقد شددت اللجنة الوطنية لتكنولوجيا المعلومات والحريات الفرنسية(CNIL) على أن المفاتيح العامة من المحتمل أن تشكل بيانات شخصية بموجب اللائحة العامة لحماية البيانات[٣].

---

[1] - Florence Chafiol. op cit n° 2

[2] - Décis. de l'ACPR rendue le 30 mars 2017, LEMON WAY, Procédure n° 2016-05.

[3] - Commission Nationale de l'Informatique et des Libertés (06 November 2018) Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data.
https://www.cnil.fr/en/blockchain-and-gdpr-solutions- responsible-use-blockchain-context-personal-data

كل مستخدم لديه مفتاح عام (سلسلة من الحروف ، والأرقام التي تمثل المستخدم)، والذى يمكن اعتباره بمثابة رقم حساب تتم مشاركته مع الآخرين لتمكين المعاملات. بالإضافة إلى ذلك، يحمل كل مستخدم مفتاحًا خاصًا (أيضًا سلسلة من الأحرف ، والأرقام)، والذي يعد كلمة مرور لا يجب مشاركتها مع الآخرين أبدًا.

كلا المفتاحين لهما علاقة رياضية يستطيع بموجبها المفتاح الخاص فك تشفير البيانات التي تم تشفيرها من خلال المفتاح العام.

بالتالي فإن المفاتيح العامة تخفي هوية الفرد ما لم يتم ربطها بمعرفات إضافية. وهذا بالطبع هو الحال فقط عندما يتعلق المفتاح العام بشخص طبيعي[١].

في الواقع، فإن المفتاح العام – مثل عنوان IP – على الرغم من أنه لا يسمح بالتعرف المباشر على الشخص المعني، إلا أنه من المرجح أن يوفر، بشكل غير مباشر، هوية الشخص المعني ، وذلك، إما عن طريق استخدام الوسائل التقنية الحالية (عن طريق تتبع البرامج مثل التحليل التسلسلي ، أو مفتش البلوك تشين)، أو عن طريق أطراف ثالثة قادرة على الكشف عن هوية الأشخاص المعنيين للسلطات (لا

[1] - Michele Fink, Blockchains and Data Protection in the European Union, Max Planck Institute for Innovation and Competition Research Paper No. 18-01Juillet 2019. P.26.

سيما المنصات المنظمة التي يجب أن تحدد هوية عملائها بموجب قوانين مكافحة الإرهاب- التزامات غسل الأموال)[١].

بخصوص "**بيانات المعاملات**" وهي المصطلحات المستخدمة للإشارة إلى فئات أخرى من البيانات التي يمكن استخدامها في سلاسل الكتل ، ولكنها ليست مفاتيح عامة.

هذه بيانات حول المعاملة في حد ذاتها. وفقًا اللجنة الوطنية لتكنولوجيا المعلومات والحريات الفرنسية ، تشير هذا إلى البيانات "الواردة" ضمن "معاملة ما (على سبيل المثال: الدبلوم ، أو سند الملكية)"[٢]يمكن أن تكون البيانات الشخصية الخاصة بالمعاملة اسمًا ، أو عنوانًا ، أو تاريخ ميلاد موجود في معاملة معينة.

هذه البيانات المتعلقة بمحتوى المعاملة قد تظهر في شكل نص عادي، أو تكون مشفرة، أو مجزأة (تظهر بصمة البيانات فقط في السجل، ويتم الاحتفاظ بالبيانات العادية خارج البلوك تشين) ، أو روابط تشير إلى خوادم خارجية.

لتحديد ما إذا كانت بيانات المعاملات تلبي تعريف اللائحة العامة لحماية البيانات للبيانات الشخصية، يجب إجراء تحليل كل حالة على حدة.

---

[1] - Thibault Verblest, op.cit.p39.

[2] - Commission Nationale de l'Informatique et des Libertés (06 November 2018) Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data. https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data

في كثير من الأحيان لن تكون بيانات المعاملات مؤهلة كبيانات شخصية. على سبيل المثال، في البيتكوين، لا يرتبط مبلغ البيتكوين المحول بالضرورة بشخص يمكن تحديده، ولا ينطبق ذلك على بيانات الدفع الخاصة بالتسوية الشاملة في نهاية اليوم بين البنوك[١]. كذلك الحال عندما تكون سلاسل الكتل بمثابة بنية تحتية للبيانات تُستخدم لمشاركة بيانات أجهزة الاستشعار المناخية من الفضاء الخارجي بين المشاركين، فهذه لا تكون بيانات شخصية[٢]. علاوة على ذلك، من غير المرجح أن تكون الأصول المشفرة المنقولة من أ إلى ب مؤهلة كبيانات شخصية ما لم يتم دمجها مع معلومات إضافية تحدد المنتج ، أو الخدمة التي تم شراؤها، مما قد يؤدي إلى تحديد الهوية[٣].

في بعض الأحيان، ستكون هذه البيانات مؤهلة على أنها بيانات شخصية. ففي بعض حالات الاستخدام الأخرى، يمكن ربط موضوع المعاملة بهويات العالم الحقيقي .على سبيل المثال، يمكن لمجموعة من بنوك التجزئة إنشاء منصة البلوك تشين لمشاركة بيانات "اعرف عميلك" الخاصة بعملائها مع بعضهم

[1] - Jean Bacon, Johan David Michels, Christopher Millard & Jatinder Singh, Blockchain Demystified: A Technical and Legal Introduction to Distributed and Centralised Ledgers, 25 Rich. J.L. & Tech., no. 1, 2018 n° 120.
[2] - Michele Fink, op cit p.28.
[3] - Jean Bacon and al (2018), op cit. n° 122.

البعض[١]. في هذه الحالة، سيكون موضوع المعاملات عبارة عن معلومات حول الأشخاص الطبيعيين ويمكن كتابتها في البلوك تشين.

وقد أكدت اللجنة الوطنية لتكنولوجيا المعلومات والحريات الفرنسية أنه" عندما تتعلق هذه البيانات بأشخاص طبيعيين، ربما غير المشاركين، الذين قد يكونون بشكل مباشر ، أو يتم تحديدها بشكل غير مباشر، وتعتبر هذه البيانات بيانات شخصية"[٢].

فيما يتعلق بالبيانات الوصفية، وهي البيانات التي تصف البيانات ، أو مورد آخر. فإذا كان مستخدمو المنصة أشخاصًا طبيعيين، فقد يتم اعتبار عناوين المرسل والمستلم بيانات شخصية. يكون هذا أكثر وضوحًا عندما تكشف هذه العناوين بشكل مباشر عن هوية الشخص بالنسبة لتطبيقات محددة.

على سبيل المثال بلوك تشين تسجيل الأراضي، قد يتم نقل سندات الملكية من فرد مسمى إلى آخر . في حين أن مشغل المنصة قد يختار استخدام أسماء مستعارة للبيانات، عن طريق استبدال اسم الشخص باسم مستعار، فإن اللائحة

[1] - Michele Fink, op cit p.28

[2]- Commission Nationale de l'Informatique et des Libertés (06 November 2018) Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data. https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data

العامة لحماية البيانات توضح أن هذه البيانات ذات الأسماء المستعارة ستظل مؤهلة كبيانات شخصية[١].

كما قد تكشف البيانات الوصفية عن نمط من المعاملات مع عناوين معروفة بشكل عام (مثل التجار) ، والتي يمكن استخدامها لتمييز مستخدم فردي من خلال تقنية تعرف باسم تحليل الرسم البياني للمعاملة . على سبيل المثال، إذا كان مطعم معين يقبل عملة البيتكوين كوسيلة للدفع وكان عنوانه معروفًا للعامة، فإن الدفعات إلى هذا العنوان تشير إلى أن المرسل زار هذا المطعم في وقت معين؛ نظرًا لهذا، قد تكون عناوين البيتكوين ، والمفاتيح العامة مؤهلة في ظروف معينة كبيانات شخصية[٢].

[1] - Jean Bacon and al (2018 op cit. n° 116

[2] - Adam Ludwin, How Anonymous Is Bitcoin?, Coin Ctr. (Jan. 20, 2015) https://coincenter.org/entry/how-anonymous-is-bitcoin. [https://perma.cc/4RTP-AMJY].

المبحث الثالث

حماية حقوق صاحب البيانات الشخصية في البلوك تشين.

تخصص المواد من ١٥ إلى ٢٢ من اللائحة العامة لحماية البيانات العديد من الحقوق المحددة لأصحاب البيانات.

يلتزم مراقبو البيانات بتسهيل ممارسة هذه الحقوق ولا يمكنهم تفويض هذه المهمة إلى المعالجين.

مراقب البيانات هو الشخص الذي يتولى واجب احترام النصوص التشريعية والتنظيمية لحماية البيانات[١]، ويتم تعريفه بأنه الشخص الطبيعي ، أو الاعتباري ، أو السلطة العامة ، أو الوكالة أو أي هيئة أخرى تحدد، بمفردها ، أو بالاشتراك مع آخرين ، أغراض ووسائل معالجة البيانات الشخصية ؛ عندما يتم تحديد أغراض ووسائل هذه المعالجة بموجب القانون[٢].

بفحص حقوق أصحاب البيانات المختلفة الواردة باللائحة العامة لحماية البيانات ، سيتبين أن البعض لا يثير أي مشاكل محددة في سياق تقنية البلوك تشين في حين أن البعض الآخر يثير تحديات فنية ، وقانونية على حد سواء.

[1] - Thibault Verblest, op.cit.p39.
[2] - GDPR Art 4(7)

بالطبع، كما هو الحال دائمًا، لا يمكن تقييم تطبيق حقوق أصحاب البيانات المختلفة هذه على البلوك تشين بشكل شامل إلا على أساس تحليل كل حالة على حدة ، والذي يأخذ في الاعتبار الظروف الفنية ، والسياقية المحددة لكل عملية معالجة بيانات شخصية.

يتم النظر في البيانات الشخصية بموجب القانون من منظور حمايتها. فهي جزء من الحياة الخاصة ، وتنتمي إلى حقوق الشخصية. من خلال إدراكنا للبيانات الشخصية للفرد، فإننا نميل إلى الاقتراب من جوهره: خصائصه الجسدية، أو وضعه الاجتماعي، أو صورته، أو عاداته الاستهلاكية، أو حتى سمعته.

إن الحق في حماية البيانات، يشبه الحق في تقرير المصير المعلوماتي، يعمل على تزويد الفرد بالتحكم في المخاطر التي يتعرض لها في العالم الرقمي[١].

تشكل حماية البيانات الشخصية حقا على المستوى الأوروبي، حيث يتم ضمان حماية البيانات الشخصية بموجب المادة ٨ من الاتفاقية الأوروبية لحقوق الإنسان، وبشكل أكثر دقة بموجب المادة ٨ من الميثاق الأوروبي للحقوق الأساسية.

حدد المشرع الأوروبي في اللائحة العامة لحماية البيانات **(GDPR)** شروط معالجة البيانات الشخصية ، وقد نصت هذه اللائحة في المادة ٢٤(١) على وظيفة جديدة

[1] - Julien Rossi op cit p.12

داخل الشركات التي تقوم بمعالجة البيانات، وهى وظيفة مسؤول الامتثال (مسؤول وحدة التحكم) الذى يجب عليه حماية البيانات ، والتأكد من الامتثال للوائح حماية البيانات نيابة عن مراقب البيانات. وهو شبيه بمسؤول الامتثال داخل البنك الذى يضمن امتثال عمليات البنك للوائح الوطنية والدولية[1].

اذا كان البلوك تشين عبارة عن سجل، "قاعدة بيانات" كبيرة تتمتع بخصوصية المشاركة في وقت واحد مع جميع مستخدميها، وجميعهم يمتلكون هذا السجل أيضًا ، فإننا ندرك أنه يجب تخطيط البلوك تشين كسجل شفاف ، وغير قابل للانتهاك ، ويتم التحكم فيه من قبل جميع مستخدميه بهدف تنفيذ عملية قانونية محددة.

هذه التكنولوجيا هي جزء من التطور المجتمعي الذي يميل إلى تعزيز تبادل المعلومات ، وينعكس هذا التطور في ظهور الشبكات الاجتماعية، أو البرمجيات مفتوحة المصدر، أو شبكات الند للند.

يظل صحيحًا أن استخدام هذه التكنولوجيا يمكن أن يتضمن بيانات شخصية، بشكل مباشر ، أو غير مباشر. في تطبيقها العملي، و لا يمكن لتقنية البلوك تشين أن تحجب هذا الحق الأساسي في حماية بيانات الأشخاص المعنيين ، والأكثر من ذلك،

[1] - PRAZ EMILIE M., Responsabilités et outils de conformité selon la RGPD, PJA 2018, p. 609

أنه من مصلحة الجهات الفاعلة التي تدافع عن فوائدها أن تثبت أن هذه الآلية جديرة بالثقة.

إذا كان يجب أن تحتوي تقنية البلوك تشين على معلومات شخصية ، فإن رد فعلها الأول سيكون مشاركتها.

تشكل شفافية المعلومات التي يستضيفها المشروع الأصلي للبلوك تشين هدفا أساسيا وبدون الشفافية، وبدون المشاركة، وبدون النشر على أكبر عدد ممكن من الأشخاص، تفقد تقنية البلوك تشين قدرتها على ضمان سلامة المعلومات للجميع.

يريد البلوك تشين مشاركة المعلومات، ويريد القانون العام لحماية البيانات (GDPR) حمايتها ، وهذه هي المفارقة القانونية الأولى بين البلوك تشين ، واللائحة العامة لحماية البيانات[1].

كذلك فإننا إذا كنا نحتاج إلى أطراف ثالثة موثوقة لضمان تبادل السلع ، أو القيم ، أو المعلومات ، كما هو الحال حيث يضمن كاتب العدل الملكية العقارية لكل شخص، وسيضمن البنك تبادل القيم ، وستقوم شبكة اجتماعية بنقل تبادل المعلومات، وما إلى ذلك. إلا أن تقنية البلوك تشين تقرر أنها تمنع المركزية ، وبالتالي لن يكون هناك حاجة لتكليف طرف ثالث موثوق به بمهمة التصديق على هذه التبادلات ، حيث يتم

[1] - Audrey SIDE op. cit p.11.

مشاركتها بين جميع مستخدميها، وبالتالي يمكن لتقنية البلوك تشين نفسها أن تضمن صحة المعلومات المرسلة ، ومن ثم تصبح عمليات التبادل أقل تكلفة وأسرع.

من جانبها، تولي اللائحة العامة لحماية البيانات أهمية كبيرة للشخص المسؤول عن معالجة البيانات الشخصية، ذلك أنه موضوع اهتمام كل اللوائح ، حيث إن التزاماته عديدة ، وتمتد مسؤوليته إلى مسؤولية المقاول من الباطن.

مثلما لا يمكن أن تكون هناك حماية للبيانات الشخصية دون بيانات شخصية، لا يمكن أن تكون هناك حماية للبيانات الشخصية دون مراقب البيانات ، واللائحة العامة لحماية البيانات (GDPR) من خلال تحديد جهة التحكم في البيانات ، والشخص المسؤول عن المعالجة يجعل البلوك تشين فاعلًا رئيسيًا ، وهذه هي المفارقة القانونية الثانية[١].

مع ذلك، فإن تقنية البلوك تشين العامة، باعتبارها أداة لا مركزية، تجعل من الصعب أو حتى من المستحيل تحديد الشخص المسؤول عن معالجة البيانات الشخصية.

[1] - Audrey SIDE op.cit p.12.

لمعالجة عدم التوافق الكبير بين البلوك تشين العامة واللائحة العامة لحماية البيانات، يقترح بعض المؤلفين اعتبار الشخص الذي يقف وراء التطبيق ، أو العقد الذكي مسؤولاً عندما يكون من الممكن التعرف على هذا الشخص[١].

ترى اللجنة الوطنية لتكنولوجيا المعلومات والحريات الفرنسية(CNIL) أن مراقبي البيانات يمكن أن يكونوا مستخدمي البلوك تشين عندما يقدمون عملية للقاصرين[٢].

على العكس من ذلك، إذا تم اعتبار أن الجهات الفاعلة في البلوك تشين ليس من اختصاص اعتبارهم مسؤولين عن المعالجة، فسيكون من الممكن أيضًا إسناد هذا الدور إلى المواقع التي تستضيف البلوك تشين[٣].

على العكس من ذلك، في البلوك تشين الخاص، يمكن تسمية مراقب البيانات ، حيث تتم إدارته من قبل سلطة يمكنها تنفيذ المتطلبات التي يفرضها القانون العام لحماية البيانات[٤].

المفارقة القانونية الثالثة هي بخصوص احترام حقوق صاحب البيانات(المستخدم) على بياناته الشخصية[١]، حيث تقدم اللائحة العامة لحماية البيانات الحق في تصحيح

[1]- Canter, Le conservatisme de la protection des données face à la révolution blockchain, in: cognitio 2019/1. P.11.
https://cognitio-zeitschrift.ch/index.php/cognitio/article/view/927 (URL)
[2] - CNIL, Premiers éléments d'analyse de la CNIL– Blockchain, septembre 2018, p. 2.
[3] - Canter, op cit p.11
[4] - Canter, op cit p.10

بياناته الشخصية ، والحق في محوها(النسيان) ، والحق في نقل المعلومات كونها تتعارض في جوهرها مع نظام البلوك تشين غير القابل للتغيير[٢].

من جانبها، تولي اللائحة العامة لحماية البيانات أهمية كبيرة للاحتفاظ المحدود بالبيانات ، والتي يجب حذفها عندما تصبح غير ذات أهمية مباشرة للشخص الذي يحتفظ بها.

علاوة على ذلك، تضمن هذه اللائحة لمالك البيانات الشخصية الحق في الوصول إلي بياناته ، وتصحيحها ، وحتى حذفها كذلك. ويخضع هذا الحق لأحكام عديدة تتعلق بمبادئه، وعمله، وربما عقوباته[٣].

من ناحية أخرى في البلوك تشين لا يمكننا إزالة جزء واحد من المعلومات الموجودة في السلسلة دون تفكيك جميع المعلومات الأخرى ، حيث يحدد مكان كل جزء من المعلومات الوجود الحقيقي لجميع المعلومات الأخرى ؛ وذلك لأن المعلومات الموجودة في البلوك تشين هي كل لا يتجزأ. ولا يمكن تزويرها، أو تصحيحها ، أو محوها. إنه مبدأ الثبات الذي تضعه البلوك تشين.

---

[١] – المادة الثانية من قانون حماية البيانات المصرى رقم ١٥١ لسنة ٢٠٢٠.

[2] - Cédric Strub ,op.cit.p.30

[3] - Audrey Side op.cit.p.12.

كذلك فإن اللائحة العامة لحماية البيانات (GDPR) تحظر نقل البيانات خارج الاتحاد الأوروبي إلا بشروط محددة للغاية ، ومع ذلك، في ظل تكنولوجيا البلوك تشين التي يمكن فيها للقاصرين أن يتواجدوا في أي مكان في العالم دون أن يكونوا معروفين بالضرورة، يمكن أن تشكل هذه النقطة تحديًا حقيقيًا يحول دون الامتثال لهذه الشروط[١].

أحد الحلول المقترحة في محاولة للتوفيق بين البلوك تشين ومتطلبات اللائحة العامة للبيانات بخصوص حقوق المستخدم على بياناته هو وجود نظامين متوازيين: البلوك تشين وقاعدة البيانات الكلاسيكية. وبهذه الطريقة، يمكن للبيانات الموجودة في قاعدة البيانات الكلاسيكية أن تلبي متطلبات اللائحة العامة لحماية البيانات.

مع كل معاملة جديدة، يتم إنشاء معرف المعاملة من أجل تحديد هذه المعاملة في نظام قاعدة البيانات. سيتم تخزين هذا المعرف على البلوك تشين ، مما يجعل من الممكن تأمين الوصول إلى البيانات، حيث أن المعرف خاص بحزمة البيانات. يضمن هذا النظام الحق في النسيان، حيث يمكن حذف البيانات من قاعدة البيانات[٢].

[1] - LE Roux Corentin, Protection des données personnelles : Impact du RGPD sur les blockchains dans le secteur de la santé,Mémoire de MASTER 1 MIAGE, Université Paris 1 Panthéon – Sorbonne 2020/2021 p.27.
[2] - Cédri Strub ,op.cit.p.31.

أمام كل هذه المفارقات القانونية بين البلوك تشين ، ومتطلبات اللائحة العامة للبيانات بخصوص حقوق المستخدم على بياناته سوف نستعرض في هذا المبحث بالتفصيل حقوق المستخدم على بياناته الشخصية وذلك على النحو التالي:

المطلب الأول

حق مستخدم البلوك تشين في الوصول لبياناته الشخصية

وفقًا للمادة ١٥ من اللائحة العامة لحماية البيانات يحق لصاحب البيانات الحصول على تأكيد من وحدة التحكم بشأن ما إذا كانت البيانات الشخصية المتعلقة به قيد المعالجة أم لا، وفي هذه الحالة، الوصول إلى البيانات الشخصية والمعلومات التالية: أغراض المعالجة، وفئات البيانات الشخصية المعنية ، المستلمون أو فئات المستلمين الذين تم الكشف عن البيانات الشخصية لهم ، أو سيتم الكشف عنها، ولا سيما المستلمون في بلدان ثالثة ، أو منظمات دولية ، حيثما أمكن، الفترة المتوقعة التي سيتم تخزين البيانات الشخصية لها، أو، إذا لم يكن ذلك ممكنًا، المعايير المستخدمة لتحديد تلك الفترة.....

في الحقيقة ليس من قبيل المصادفة أن قائمة الحقوق المختلفة لأصحاب البيانات تبدأ بحقه فى الوصول لبياناته الشخصية.

يجب اعتبار حق الوصول حقًا أساسيًا في قانون حماية البيانات الأوروبي ؛ نظرًا لأنه يمكّن، وغالبًا ما يكون شرطًا أساسيًا، لممارسة أي من الحقوق الأخرى لصاحب البيانات.

في الواقع، فإن الوصول إلى البيانات الشخصية يمكّن صاحب البيانات من فهم البيانات التي تتم معالجتها بواسطة مراقب البيانات، والتي قد تكون خطوة أولى ضرورية قبل ممارسة أي حق آخر، حيث يلعب حق الوصول دورًا محوريًا في تمكين حقوق البيانات الأخرى ، ومراقبة الامتثال ، وضمان الإجراءات القانونية الواجبة ، فهو شرط أساسي لتصحيح ، أو مسح أو حجب البيانات، وبالتالي فإن وجود (ومدى) حق الوصول يجب أن يسمح بالاستخدام الفعال لحقوق البيانات الأخرى[1].

وبالتالي فإن المادة ١٥ من القانون العام لحماية البيانات تكون قد وضعت حقا تمكينيا له أهمية كبيرة بالنسبة للهيكل العام لقانون حماية البيانات الأوروبي.

بشكل عام، لا توجد عقبات مبدئية تمنع تنفيذ المادة ١٥ من اللائحة العامة لحماية البيانات فيما يتعلق بسلاسل الكتل. ومع ذلك، فإن هذا يفترض وجود آليات حوكمة مناسبة تتيح التواصل الفعال وإدارة البيانات.

[1] - Case C 434/16 Peter Nowak v Data Protection Commissioner EU:C:2017:994 - Case C-553/07 College van burgemeester en wethouders van Rotterdam v MEE Rijkeboer EU:C:2009:293 .

يمكن توجيه طلبات الوصول للبيانات من قبل صاحب البيانات إلى مراقب البيانات ، أو إلى أي من المراقبين المشتركين[١].

لا يُسمح لمراقبي البيانات بإحباط أصحاب البيانات في محاولاتهم للاستفادة من المستوى العالي من الحماية الذي يترتب على حقوقهم الأساسية . ففي الواقع، يتعين عليهم تنفيذ حقوق أصحاب البيانات ، وكذلك تسهيل ممارسة هذه الحقوق[٢].

إن مراقبي البيانات لا يمكنهم تقييد حق الوصول للبيانات من خلال تنسيق ملف غير عادل، وقيود النطاق، والاستجابة النموذجية، بل يجب عليهم عندما تكون مجموعات البيانات معقدة تسهيل الأدوات لتمكين الفهم. مع ذلك فإن حماية البيانات يجب أن تُفهم ضمن إطار مسؤوليات و صلاحيات ، وقدرات مراقب البيانات[٣].

في ضوء اللائحة الأوروبية، تتوافق كل معالجة للبيانات الشخصية مع مراقب البيانات، المسؤول عن تنفيذ التدابير الفنية والتنظيمية المناسبة ؛ لضمان القدرة على إثبات أن المعالجة تتم وفقًا للوائح المذكورة[٤].

لا يزال من الضروري معرفة من هو المتحكم في البيانات. خاصة وأن هذه الاستجابة تبدو غير متسقة فيما يتعلق ببروتوكولات البلوك تشين الأساسية المختلفة.

---

[1] - GDPR Art 26(3)
[2] - GDPR, art 12(2).
[3] - Jef Ausloos, Micheal Veale and René Mahieu, Getting Data Subject Rights Right, 10 (2019) JIPITEC. P.284
[4] - GDPR Art. 24(1)

عندما يتعلق الأمر بمنصات التبادل التي تجمع البيانات الشخصية وتعالجها، فإنهم– وليس القُصَّر (الذين يجعلون ببساطة قدراتهم الحاسوبية متاحة للشبكة)– هم الذين سيتم تعيينهم كمراقبين للبيانات.

قد يُطرح السؤال حول ما إذا كان بإمكاننا أن نتصور، في سياق البلوك تشين العام، المسؤولية المشتركة عن المعالجة بين جميع أعضاء الشبكة(العُقد) ؛ ومع ذلك، فإن تعدد المشاركين يجعل من المشكوك فيه ما إذا كان لهذه المسؤولية المشتركة أي معنى في الممارسة العملية ، خاصة وأنه لا يمكن فرض أي عقوبة مالية محتملة في هذا النوع من الظروف.

واقعيا فإن هذه العُقد التي قد تكون مؤهلة كوحدات تحكم (مشتركة) بموجب اللائحة العامة لحماية البيانات قد تكون غير قادرة فعليًا على الوصول إلى البيانات الموجودة على البلوك تشين ، حيث إنها ترى من حيث المبدأ فقط البيانات المشفرة والمجزأة حين يتم تعديل البيانات عند وضعها على البلوك تشين ؛ ونتيجة لذلك، قد لا تتمكن هذه الجهات الفاعلة من تحديد ما إذا كان البلوك تشين يحتوي بالفعل على بيانات شخصية تتعلق بصاحب البيانات الذي يبدأ الحق في الوصول لبياناته[1].

[1] - Michele Fink, op cit p.72

بالنسبة إلى البلوك تشين الخاص، يكون من الأسهل تحديد وحدة التحكم في البيانات حيث يمكن أن تُنسب إلى مصمم البروتوكول ، أو إلى مدير البلوك تشين الخاص[١].

المطلب الثاني

الحق في تصحيح البيانات الشخصية

وفقًا للمادة ١٦ من اللائحة العامة لحماية البيانات يحق لصاحب البيانات الحصول من المراقب دون تأخير غير مبرر على تصحيح البيانات الشخصية غير الدقيقة المتعلقة به. مع الأخذ في الاعتبار أغراض المعالجة. كما يحق لصاحب البيانات إكمال البيانات الشخصية غير المكتملة عن طريق تقديم بيان تكميلي.

المقصود من حق التصحيح أن يتم ممارسته في حالة وجود خطأ في التسجيل الذي تم إجراؤه على البلوك تشين ، أو في البيانات الخارجية عنه والتي تم تسجيل بصمتها على البلوك تشين.

يجب أن يكون التصحيح مبررًا فيما يتعلق بأغراض المعالجة، مما يحد من ممارسة هذا الحق. ومع ذلك، لا يمكن تعديل التسجيل الأولي، مما يبطل حق التصحيح[٢].

[1] - Florence Chafiol op cit.
[2] - Thibault Douville op cit n° 11.

للوهلة الأولى، يبدو أن هذه الحقوق تتعارض مع "ثبات" تقنية البلوك تشين ، ومع ذلك، فإن القدرة على الامتثال لمثل هذه الطلبات تختلف اعتمادًا على تصميم منصة البلوك تشين.

بخصوص منصات البلوك تشين المركزية سنجدها تدعم إمكانية التصحيح بشكل أفضل ؛ حيث يمكنها أن تحد من رؤية السجل لأطراف معينة ، ونتيجة لذلك، سيكونون في وضع أفضل للامتثال لطلبات أصحاب البيانات لتصحيح أو حتى مسح البيانات في الكتل السابقة ، وذلك مرهون بأن يكون مشغلو المنصات المركزية قادرين على الامتثال لطلبات المحو[١].

على سبيل المثال، إذا طلب مستخدم من البنوك تصحيح جزء معين من المعلومات في سجل عملائه على البلوك تشين ، فيمكن لكل بنك الامتثال عن طريق تغيير سجل المعاملة ذي الصلة ، وإعادة تجزئة الكتل اللاحقة في نسخته من دفتر الأستاذ.

أما بخصوص منصات البلوك تشين المفتوحة والموزعة ، فالحقيقة أن هذا الحق في التصحيح سيشكل مشكلة بالنسبة لها؛ ذلك أنه يتعارض بشكل أساسي مع متطلبات اللائحة العامة لحماية البيانات بأن تكون البيانات قابلة للتغيير ؛ حيث إن البلوك تشين عبارة عن دفتر أستاذ للإلحاق فقط ، وغالبًا ما يكون مصممًا بشكل هادف

[1] - Jean Bacon and al (2018), op cit . n° 161

لجعل حذف البيانات وتعديلها مرهقًا للغاية من أجل تأمين سلامة البيانات ، والثقة في الشبكة.

إذا كان يمكن للعقدة طالبة التصحيح تغيير نسختها ، إلا أنه من غير الواضح كيف سيلتزم المشاركون الفرديون الآخرون- سواء كان أحد العقد ، أو المُعدن- بهذه الطلبات.

واقعيا لا يمكن لسلاسل الكتل في كثير من الأحيان أن تدعم إمكانية الرجوع. فعلى سبيل المثال عندما يطلب العميل الذي يستخدم سلسلة الكتل من مزود الخدمة تصحيح المعلومات في سجله[١]. يمكن أن تدعم سلاسل الكتل الخاصة ، أو غير المسموح بها مثل هذه الطلبات من خلال تغيير سجل المعاملات ذي الصلة عن طريق إعادة تجزئة الكتل اللاحقة حيث يتم تسهيل ذلك من خلال الإعداد الفني والحوكمة[٢].

بخصوص سلاسل الكتل العامة من الناحية النظرية، يمكن لجميع العقد الاتفاق على "فرع" لإصدار جديد من البلوك تشين بشكل دوري ؛ لتعكس طلبات التصحيح .

[1] - Michele Fink, op cit p.72
[2] - Ibid.

ومع ذلك، من الناحية العملية، قد يكون من الصعب تحقيق هذا المستوى من التنسيق بين آلاف العقد المحتملة[١].

مع ذلك، تنص المادة ١٦ من اللائحة العامة لحماية البيانات صراحةً على خيار إكمال البيانات غير الكاملة "عن طريق تقديم بيان تكميلي"، ويعد هذا أسهل بكثير في التنفيذ فيما يتعلق بدفاتر الأستاذ الموزعة حيث يمكن لأي طرف لديه حقوق الكتابة إضافة بيانات جديدة إلى دفتر الأستاذ الذي يصحح المعلومات السابقة.

على سبيل المثال، عندما تعكس سجلات المستخدم أنه عازب، يمكن إضافة بيانات إضافية إلى كتلة جديدة للإشارة إلى أن هذا لم يعد هو الحال بعد زواج جديد[٢].

مع ذلك، فمن الجدير التساؤل عما إذا كانت إضافة معلومات جديدة على السلسلة ستكون في جميع الظروف وسيلة مرضية لتحقيق الأساس المنطقي المتأصل في المادة ١٦ من اللائحة العامة لحماية البيانات؟.

باعتماد هذا النهج الهادف، يبدو من الواضح أن تقديم بيان تكميلي قد لا يكون دائمًا وسيلة مرضية لتحقيق الامتثال للحق في التصحيح، كما هو الحال عندما تكون هناك حجة قوية مفادها أنه لا ينبغي مجرد استكمال البيانات بل إزالتها واستبدالها (كما هو الحال في السيناريوهات التي لا يستطيع فيها صاحب البيانات الاعتماد على حق

[1] - Jean Bacon and al (2018), op cit . n° 162
[2] - Michele Fink, op cit p.73.

المحو حيث لا ينطبق أي من الأسباب الواردة في المادة ١٧ (١) من اللائحة العامة لحماية البيانات[١].

على العكس من ذلك، يمكن القول: "أنه حيث لا تنطبق المادة ١٧ (١) من اللائحة العامة لحماية البيانات، فإنه لا يمكن اعتبار صاحب البيانات مهتمًا بمحو البيانات، وأن مجرد تقديم معلومات إضافية يجب أن يعتبر كافيًا".

بالإضافة إلى تغيير السلسلة، قد تكون هناك أيضًا أساليب فنية أخرى للمساعدة في الامتثال لحماية البيانات .على سبيل المثال، قد لا يتطلب تطبيق البلوك تشين تخزين البيانات الشخصية على السلسلة، بل يوفر روابط لهذه البيانات الموجودة خارجيًا[٢].

[1] - Ibid.

[2] - Jean Bacon and al (2018)op. cit n° 163 - Guy Zyskind ,Oz Nathan and Alex 'Sandy, Decentralizing Privacy: Using Blockchain to Protect Personal Data, 2015 IEEE Sec. & Privacy Workshops 180, 181

المطلب الثالث

الحق في محو البيانات الشخصية ("الحق في النسيان")[١]

يحق لصاحب البيانات أن يحصل من المراقب على محو البيانات الشخصية المتعلقة به دون تأخير غير مبرر، ويكون المراقب ملزمًا بمحو البيانات الشخصية دون تأخير غير مبرر عندما يتوافر لدي صاحب البيانات أسباب مشروعة في المحو وفق المادة ١٧ من اللائحة العامة لحماية البيانات.

يجب على المراقب، مع الأخذ في الاعتبار التكنولوجيا المتاحة ، وتكلفة التنفيذ، اتخاذ خطوات معقولة، بما في ذلك التدابير الفنية ؛ لإبلاغ المراقبين الذين يقومون بمعالجة البيانات الشخصية بأن صاحب البيانات قد طلب مسح أي وحدات تحكم من قبل هؤلاء المراقبين ، أو روابط إلى تلك البيانات الشخصية ، أو نسخها ، أو تكرارها.

[١] – ومن المجالات المحددة المثيرة للقلق في هذا الصدد البيانات "المحذوفة . "في العديد من التطبيقات الشائعة لبرامج قواعد البيانات، فإن عملية المعالجة التي يشار إليها عادةً باسم "الحذف" تؤدي فقط إلى تغيير التسمية المرفقة بنقطة البيانات .على سبيل المثال، ربما قام أحد الأشخاص بالضغط على زر "حذف" في منشور على وسائل التواصل الاجتماعي، أو قد يبدو العنوان القديم "محذوفًا" عند الكتابة فوقه بعنوان جديد، ولكن هذا لا يعني بالضرورة حذف البيانات المرتبطة من خوادم وحدة التحكم . وفي حين أن هذه الممارسة قد تكون مناسبة، حسب الظروف، فمن المهم التأكيد على أن هذه البيانات لا تزال موجودة في النظام، وبالتالي تقع ضمن نطاق حق الوصول إلى البيانات الشخصية. Jef Ausloos, Micheal Veale and René Mahieuop. cit. P.287

١١ - حماية البيانات الشخصية عبر تقنية البلوك تشين

يعد الحق في محو البيانات أداة مهمة نحو مزيد من تقرير المصير المعلوماتي ؛ لأنه يوفر لصاحب البيانات التحكم في البيانات الشخصية التي تتعلق به بشكل مباشر ، أو غير مباشر[١].

في الواقع، أثبتت الأبحاث المهمة في العلوم السلوكية أن أصحاب البيانات المتصور لديهم سيطرة على بياناتهم الشخصية من خلال أدوات مثل الحق في المحو، قد يؤدي بشكل متناقض إلى تقليل المخاوف بشأن ممارسات معالجة البيانات ، والشعور الزائف بالأمان، والذي بدوره قد يؤدي إلى الكشف عن المزيد من المعلومات (الحساسة)[٢].

تمكن المادة ١٧ من اللائحة العامة لحماية البيانات أصحاب البيانات من الحصول على "محو" البيانات الشخصية من مراقب البيانات إذا انطبق أحد الأسباب المذكورة.

في الواقع، فإن حق المحو هو حق مشروط ومحدود في نفس الوقت ، ولا يمكن الاحتجاج به إلا وفقًا للشروط الواردة في المادة ١٧ (١) من اللائحة العامة لحماية البيانات ، ويجب علاوة على ذلك موازنته مع الاعتبارات الواردة في المادة ١٧ (٢) من اللائحة العامة لحماية البيانات. علاوة على ذلك، فإن الحق في المحو ليس سوى حل أخير، حيث يمكّن أصحاب البيانات من طلب المحو في المواقف التي يجب أن يتم فيها محو بياناتهم الشخصية بالفعل في المقام الأول.

---

[1] - Michele Fink, op cit p.75.
[2] - Jef Ausloos, Micheal Veale and René Mahieu, op. cit. P.299

إن الحق في المحو المنصوص عليه في اللائحة العامة لحماية البيانات سيكون متناقضًا تمامًا مع مبادئ تقنية البلوك تشين ذاتها، وإحدى سماتها هي أن البيانات بمجرد إدخالها لا يمكن تعديلها ، أو تغييرها لاحقًا.

وقد شدد الكثيرون على صعوبة تطبيق حق المحو على البلوك تشين ؛ وذلك لأن حذف البيانات أمرًا مرهقًا بسبب أن هذه الشبكات غالبًا ما تكون مصممة بشكل هادف لجعل التعديل الأحادي للبيانات أمرًا صعبًا، والذي بدوره من المفترض أن يولد الثقة في الشبكة من خلال ضمان سلامة البيانات ، وبالتالي فإن صعوبة الامتثال للمادة ١٧ من اللائحة العامة لحماية البيانات مثقلة بالعوامل الفنية، وأيضًا بتصميم الحوكمة[1].

بعبارة أخرى، لا يمكن ضمان أي حماية للبيانات المتبادلة إلا من خلال الثقة في تكنولوجيا البلوك تشين ، ويستند هذا إلى عدم إمكانية الرجوع عن البيانات المكتوبة في سلسلة الكتل التي تم التحقق من صحتها من قبل المشاركين.

مع ذلك، فإن المحو ممكن من الناحية النظرية من خلال آلية تفكيك العقد ، وإعادة بنائها، لكن من الناحية العملية يبدو تحقيق ذلك صعبًا للغاية.

[1] - Michele Fink, op cit p.75.

لحذف البيانات، سيتعين على أكثر من نصف عقد الشبكة العمل معًا ؛ لإعادة بناء البلوك تشين من لحظة إضافة البيانات (الأغلبية مطلوبة للبلوك تشين العامة).

تخيل أنه تم العثور على بلوك تشين يحتوي على أسماء وعناوين الأطفال المعرضين لخطر سوء المعاملة (نختار عمدًا شيئًا يقول معظم الناس إنه لا ينبغي أن يكون متاحًا للعامة).

لمسح هذه البيانات، سيتعين على أكثر من نصف العقد التي تحافظ على البلوك تشين أن تعمل معًا لإعادة بناء البلوك تشين منذ إضافة تلك البيانات.

تشبه هذه العملية إعادة البناء من نسخة احتياطية: أثناء إعادة البناء، سيتم إعادة إلى حالة سابقة ، أيام ، أو أسابيع ، أو حتى أقدم من ذلك بكثير.

خلال هذا الوقت (تستغرق إعادة بناء البلوك تشين بعض الوقت عمدًا) لن تكون البيانات محدثة. قد يكون هذا أيضًا وقتًا يمكن أن تتسلل فيه تغييرات غير مرغوب فيها على البيانات الجديرة بالثقة[١].

بالإضافة إلى هذا البديل المتفق عليه والذي يصعب تنفيذه، يمكن للأقلية دائمًا استدعاء الشوكة، والتي تتضمن تقسيم البلوك تشين إلى قسمين، إذا اعتقدت أنها تستطيع إجراء تحسينات على البروتوكول[١].

[1] - Open Data Institute, Applying blockchain technology in global data infrastructures, ODI-TR-2016-001, 2016, p. 17.

يوفر بروتوكول البيتكوين –عندما يعتقد المستخدمون أن بإمكانهم إجراء تحسينات على البروتوكول– إمكانية إطلاق شوكة صلبة، أي إصدار جديد من البروتوكول يقسم السلسلة إلى قسمين ويجعلها غير متوافقة مع الإصدار القديم ، وبالتالي لا يمكن أن تكون المعاملات اللاحقة جزءًا من استمرارية السلسلة.

الانقسام الأكثر شهرة هو انقسام شوكة Ethereum في يوليو ٢٠١٦. وكانت العُقد المسماة DAO بها العديد من العيوب الأمنية التي سمحت للسارق بالاستيلاء على جزء كبير من الأموال المخزنة في هذا العقد.

وبعد مناقشة طويلة وقوية انقسمت السلسلة إلى قسمين في ٢٠ يوليو ٢٠١٦. اتبع جزء من عقد إيثريوم التعليمات البرمجية التي لم تتغير (قواعد غير قابلة للتغيير)، وقام جزء آخر بتثبيت برامج معدلة، حيث منعت قاعدة جديدة اللص من استعادة حصته، وسمحت بتعويض المشاركين فيDAO.

تستمر السلسلتان حتى اليوم، إحداهما ذات قواعد لم تتغير تسمى الآن إيثريوم الكلاسيكية ، والأخرى ذات القواعد الجديدة تسمى إيثريوم [٢].

[1] - Florence Chafiol, op cit.
[2] - Stéphane Bortzmeyer, La chaîne de blocs n’est pas immutable, 12 septembre 2016.
https://www.ethereum-france.com/la-chaine-de-blocs-nest-pas-immuable.

في الواقع، حتى لو كانت هناك وسيلة لضمان الامتثال من منظور تقني، فقد يكون من الصعب من الناحية التنظيمية إقناع جميع العقد بتنفيذ التغييرات ذات الصلة على نسختها الخاصة من قاعدة البيانات (وخاصة في سلاسل الكتل العامة ، وغير المسموح بها).

يجب التأكيد على أن المعنى الدقيق لمصطلح "المحو" لا يزال غير واضح ؛ حيث إن المادة ١٧ من اللائحة العامة لحماية البيانات لم تحدد ما هو المقصود من المحو، وهل يعني "الإزالة للكتابة ،أو المواد المسجلة ،أو البيانات، أو "إزالة آثار كل شيء ؟ إذا تم الأخذ بالمنظور السابق فيمكن اعتبار المحو بمثابة التدمير، ومع ذلك، فقد تم التأكيد بالفعل على أن تدمير البيانات الموجودة على سلاسل الكتل، وخاصة تلك ذات الطبيعة العامة ليس بالأمر السهل على الإطلاق ، و لا يجب تفسيره على أنه يتطلب التدمير التام للبيانات [١].

وقد اعتبر معهد البيانات المفتوحة أن حذف البيانات أو الإغلاق الكامل لعمل العقد المطلوبة من قبل المحكمة يمكن أن يسبب أضرارًا جانبية ويغير سلسلة الكتل بأكملها؛ لأن بعض البيانات القانونية المحذوفة في الكتلة قد تكون حيوية. ويكمن الخطر في

[1] - Michele Fink, op cit p.75.

بقاء بيانات خاطئة ، أو غير كاملة على البلوك تشين ؛ لمنع تلف هذه البيانات الحيوية[١].

علاوة على ذلك، أشارت الهيئات التنظيمية الوطنية وفوق الوطنية إلى أنه قد تكون هناك بدائل للتدمير التام للبيانات التي يمكن أن تضمن الامتثال لالتزام المحو بموجب اللائحة العامة لحماية البيانات[٢].

في رأيها بشأن الحوسبة السحابية، رأت فرقة العمل المادة ٢٩ أن تدمير الأجهزة يمكن أن يكون مؤهلاً للمحو لأغراض المادة ١٧ من اللائحة العامة لحماية البيانات[٣].

علاوة على ذلك، اعتبرت سلطات حماية البيانات الوطنية الأوربية أن المحو لا يساوي بالضرورة التدمير. على سبيل المثال، أدركت هيئة حماية البيانات النمساوية مؤخرًا أن مراقب البيانات يتمتع بالمرونة فيما يتعلق بالوسائل التقنية لتحقيق المحو، وأنه يمكن اعتبار إخفاء الهوية وسيلة لتحقيق المحو طالما أنه لا يمكن التعرف على صاحب البيانات[٤].

---

[1] - Florence Chafiol op cit - Open Data Institute, op cit , p. 17.

[2] - Michele Fink, op cit p.76.

[3] - Groupe de travail Article 29 Sur La Protection Des Donnees -Avis 05/2012 sur l'informatique en nuage01037/12/FR

[٤]- في هذه الحالة المحددة، طالب أحد الأفراد بحذف بياناته الشخصية التي قدمها أثناء تقديم طلب عبر الإنترنت للحصول على عقد تأمين.

استجاب مراقب البيانات المسؤول، وهو شركة تأمين نمساوية، في الوقت المناسب وأبلغ صاحب البيانات بأن البيانات المستخدمة لأغراض التسويق سيتم حذفها بشكل لا رجعة فيه في غضون

علاوة على ذلك، فإن مكتب مفوض المعلومات في المملكة المتحدة يرى منذ فترة طويلة بأنه حيثما "وضعت البيانات خارج نطاق الاستخدام" فقد يكون هذا مرضيًا أيضًا[١].

كذلك كان للجنة الوطنية للمعلوماتية والحريات الفرنسية(CNIL) رأيها أيضا بشأن فكرة المحو. حيث رأت أنه مع تزايد الوعي بشأن التوفيق الصعب بين المادة ١٧ من اللائحة العامة لحماية البيانات و البلوك تشين تم النظر في عدد من البدائل التقنية للتدمير التام للبيانات من قبل جهات فاعلة مختلفة. واقترحت أن الحل يكمن في تدمير المفتاح الخاص، مما قد يؤدي إلى جعل البيانات المشفرة باستخدام مفتاح عام

بضعة أسابيع، بينما سيتم إخفاء هوية بعض المعلومات الشخصية الأخرى كأول مرة خطوة، فقط. وسيكون هذا مطلوبًا بسبب تبعيات نظام تكنولوجيا المعلومات المحددة.

في الواقع، تم تغيير أي معلومات شخصية إلى بيانات " وهمية " مجهولة المصدر و تم إبلاغها بشفافية إلى صاحب البيانات. ومع ذلك؛ نظرًا لأن المطالبات المستمرة من قبل صاحب البيانات بالمحو الكامل لم يتم تلبيتها من قبل مراقب البيانات – الذي استجاب بالطبع باستمرار لاحتماله السابق، لكنه لا يزال يعتمد على حججه – فقد تم تقديم مطالبة بانتهاك اللائحة العامة لحماية البيانات إلى جهاز تسوية المنازعات.

رفض جهاز تسوية المنازعات المطالبة ، وذكر أن مراقب البيانات قد استوفى بالكامل طلب صاحب الشكوى بحذف بياناته عن طريق استبعاد إمكانية تتبع الشخص. النتيجة الرئيسية للقرار هي أنه يُسمح بإخفاء الهوية بدلاً من الحذف الكامل، لأنه لا يمكن إجراء المعالجة ، أو أي استخدام آخر ؛ نظرًا لعدم وجود مرجع شخصي متبقي.

Austrian Data Protection Authority, DSB-D123.270/0009-DSB/2018 (05 December 2018)

[1] - Case C-434/16 Peter Nowak [2017] EU:C:2017:994, para 55.

غير قابلة للوصول. كما رات أنه يمكن الحصول على المحو عندما يتم حذف المفتاح السري لوظيفة التجزئة – ذات المفاتيح – مع المعلومات من الأنظمة الأخرى حيث تم تخزينها للمعالجة[١].

أما بخصوص البيانات الشخصية الموجودة على سلاسل الكتل العامة التي تتم معالجتها بواسطة منصات التبادل ، فسيتم مسحها بسهولة أكبر؛ لأنها غير مرتبطة بالبروتوكول.

وكذلك الحال بالنسبة لسلاسل الكتل الخاصة، سيكون من الأسهل أيضًا حذف البيانات الشخصية بقرار من المدير، أو بالنسبة للاتحاد، بموافقة المشاركين المعينين[٢].

يقترح تقرير المجموعة التكنولوجيا المالية الأوربية أنه من الممكن معالجة عدم التوافق هذا ، وذلك بجعل المشارك في البلوك تشين يتنازل عن حقه في المحو.

كما يقرر أنه منذ اللحظة التي يتم فيها إبلاغ صاحب البيانات بشكل واضح ومسبق أنه في حالة المشاركة في البلوك تشين ، ستصبح شروط ممارسة حقه في المحو غير

[1] - Commission Nationale Informatique et Libertés (September 2018), Premiers Éléments d'analyse de la CNIL : Blockchain, 8-9.
https://www.cnil.fr/sites/default/files/atoms/files/la_blockchain.pdf.
[2] - Florence Chafiol op cit.

قابلة للتطبيق، سيكون هذا التنازل مقبول، وسيكون له ما يبرره في الواقع فيما يتعلق بالغرض المحدد للبلوك تشين وهو الحفاظ على البيانات[١].

ويذهب هذا التقرير إلى أنه يمكن إبلاغ الشخص المعني بأن الغرض الأساسي من البلوك تشين هو الحفاظ على بيانات العمليات التي تظهر بطريقة غير قابلة للتغيير بمرور الوقت، وبالتالي ستكون البيانات ضرورية دائمًا فيما يتعلق بالأغراض التي تم جمعها من أجلها.

بعيدًا عن العملية التي ينفذها البلوك تشين ، تتعلق الموافقة بالحفظ غير القابل للتغيير للبيانات في البلوك تشين ، والضرورية لتشغيلها، وفي جميع الحالات يمكن أن تكون المصلحة المشروعة لوحدة تحكم البيانات هي أساس هذه المعالجة.

ويرى هذا النهج كذلك أن الهدف من الحق في المحو هو جعل البيانات الشخصية غير قابلة للوصول ، والنتيجة التي يمكن الحصول عليها عن طريق المحو، يمكن الحصول عليها أيضا عن طريق إخفاء الهوية بشكل لا رجعة فيه، وبمجرد أن لا يكون من الممكن تحديد هوية الفرد بشكل مباشر ، أو غير مباشر من خلال العملية التي شارك فيها، يتحقق هدف الحق في المحو؛ لذلك، إذا لم يكن من الممكن حذف

[1] - Les Impacts Dse Reseaux Distribues Et De La Technologie Blockchain Dans Les Activites De Marche Rapport Groupe Fintech Paris Europlace, 23 Octobre 2017 p.83

عملية ما، فمن المحتمل أن يتم إخفاؤها ، أو جعل البيانات الشخصية لهذه العملية غير قابلة للوصول، بشكل لا رجعة فيه[١].

ويُرد على هذا القول بأن مثل هذا التنازل عن الحق في المحو يبدو من الصعب الحصول عليه في البلوك تشين العامة، ويرجع ذلك مرة أخرى إلى عدم وجود سلطة يمكنها أن تطلب من المشاركين التنازل عن حقهم في المحو. أما في البلوك تشين الخاص، فيمكن للسلطة المنظمة القيام بذلك بسهولة، وإذا اعترض أحد الأطراف، فلن يتمكن من المشاركة في البلوك تشين[٢].

وهناك من يرى أن حق المحو هو حق محدود ومشروط في نفس الوقت، حيث توضح المادة ١/١٧ من اللائحة العامة لحماية البيانات (GDPR) ، والحيثية ٦٥ أنه لا يلزم مسح البيانات عندما يكون الاحتفاظ الإضافي بالبيانات ضروريًا للامتثال لالتزام قانوني. يعد هذا أحد الاعتبارات ذات الصلة فيما يتعلق بالعديد من حالات استخدام تقنيات البلوك تشين في المجال المالي مثل التزام الاحتفاظ بالبيانات بهدف ضمان أن تكون الأسواق المالية أكثر أمانًا وكفاءة ، وتعزيز حماية المستثمرين [٣].

[1] - Rapport Groupe Fintech Paris Europlace, 23 Octobre 2017 op cit p.84.
[2] - Canter, op cit p.12
[3] -Michele Fink, op cit p.78- Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments..

أحد الحلول المقترحة لحماية البيانات الشخصية- كما سبق القول- هو وجود نظامين متوازيين: البلوك تشين ، وقاعدة البيانات الكلاسيكية. بهذه الطريقة، يمكن للبيانات الموجودة في قاعدة البيانات الكلاسيكية أن تلبي متطلبات اللائحة العامة لحماية البيانات. مع كل معاملة جديدة ، يتم إنشاء معرف المعاملة من أجل تحديد هذه المعاملة في نظام قاعدة البيانات. سيتم تخزين هذا المعرف على البلوك تشين ، مما يجعل من الممكن تأمين الوصول إلى البيانات ، حيث أن المعرف خاص بحزمة البيانات. يضمن هذا النظام الحق في النسيان، حيث يمكن حذف البيانات من قاعدة البيانات[١].

المطلب الرابع

الحق في إمكانية نقل البيانات الشخصية

يعد الحق في إمكانية النقل أحد الابتكارات الرئيسية في اللائحة العامة لحماية البيانات مقارنة بتوجيه حماية البيانات لعام ١٩٩٥، حيث تنشئ المادة ٢٠ من اللائحة العامة لحماية البيانات حقًا جديدًا في إمكانية نقل البيانات ، وهو حق يرتبط ارتباطًا وثيقًا بالحق في الوصول إلى البيانات[٢].

[1] - Cédric Strub ,op.cit.p.31 - LE ROUX op cit p.33
[2] - Groupe de travail Article 29 (5 avril 2017), Lignes directrices sur le droit à la portabilité WP 16/EN, WP 242 rév.01, 4 p.4

يفرض القانون العام لحماية البيانات شروطًا على عمليات نقل البيانات الشخصية من الاتحاد الأوروبي إلى أي دولة خارجه، أي دولة خارج المنطقة الاقتصادية الأوروبية ، وبالتالي يجب على المراقبين التأكد من أن لديهم أساس قانوني مناسب لأي نقل دولي للبيانات.

عملاً بالمادة ٢٠ من اللائحة العامة لحماية البيانات يحق لصاحب البيانات الحصول على البيانات الشخصية المتعلقة به، والتي قدمها إلى وحدة التحكم، بتنسيق منظم ، وشائع الاستخدام ، وقابل للقراءة آليًا، وله الحق في نقل هذه البيانات إلى جهة أخرى وحدة التحكم دون عائق من وحدة التحكم التي تم تقديم البيانات الشخصية إليها.

يهدف مبدأ قابلية نقل البيانات الشخصية "إلى تمكين أصحاب البيانات فيما يتعلق ببياناتهم الشخصية ؛ لأنه يسهل قدرتهم على نقل البيانات الشخصية، أو نسخها ، أو نقلها بسهولة من بيئة تكنولوجيا معلومات إلى أخرى".٥١١ حيث يتوافق طلب صاحب البيانات لقابلية النقل مع وفقًا لمتطلبات المادة ٢٠ من اللائحة العامة لحماية البيانات، فإن وحدات التحكم ملزمة بإتاحة البيانات في "تنسيق منظم وشائع الاستخدام وقابل للقراءة آليًا".٥١٢ علاوة على ذلك، يجب أن يكون هذا في "تنسيق قابل للتشغيل البيني".

يمكن إجراء هذا النسخ الاحتياطي على جهاز خاص، أو سحابة خاصة، دون الحاجة إلى نقل البيانات إلى وحدة تحكم أخرى [١].

وفقا للمادة ١٧ من اللائحة العامة لحماية البيانات عندما يمارس شخص ما حقه في إمكانية نقل البيانات، فإنه يفعل ذلك دون التأثير على أي حقوق أخرى ، فلا تؤدي إمكانية نقل البيانات تلقائيًا إلى مسح البيانات من أنظمة وحدة التحكم ، ولا تؤثر على فترة الاحتفاظ الأولية التي تنطبق على البيانات المنقولة.

كذلك إذا كان صاحب البيانات يرغب في ممارسة حقه في محو بياناته ، فلا يمكن لوحدة تحكم البيانات استخدام إمكانية نقل البيانات كوسيلة لتأجيل ، أو رفض هذا المحو.

بخصوص تقنية البلوك تشين والتي تتكون من شبكة عامة ، ولا مركزية. في جوهر الأمر، سوف تكون البيانات الشخصية الموجودة في البلوك تشين متناثرة ، ومكررة في جميع أنحاء الكوكب.

بالتالي، لا يمكن نقل" البيانات الشخصية من البلوك تشين إلى الدول التي لا تضمن مستوى مناسبًا من الحماية من وجهة نظر القانون الأوروبي[٢].

[1] - Groupe de travail Article 29 (5 avril 2017), op. cit, 4 p.4.
[2] - Thibault Verblest, op.cit.p.40

على سبيل المثال فمن أجل تشغيل عقدة في بلد خارج الاتحاد الأوربي ، سيحتاج سجل الأراضي والبنوك إلى ضمان مستوى مناسب من الحماية ، أو الضمانات المناسبة (على سبيل المثال، عن طريق تحديد موقع العقدة في بلد خاضع لقرار كفاية اللجنة ، أو عن طريق وضع ضمانات كافية مثل شروط العقد القياسية المعتمدة)[١].

ومع ذلك، فإن المنصات المفتوحة والموزعة هي بحكم تصميمها غير مقيدة بالحدود الدولية: عادةً يمكن لأي شخص، في أي مكان، تنزيل أرشيف المعاملات بالكامل والبدء في معالجة المعاملات الجديدة كعقدة ، أو عامل تعدين ، ونتيجة لذلك من المرجح أن يستلزم استخدام هذه المنصات نقل البيانات إلى بلدان ثالثة[٢] .

وبما أن أي طرف في أي بلد ثالث يمكنه تنزيل الأرشيف، فمن غير المرجح أن توفر قرارات الملاءمة والضمانات المناسبة (بما في ذلك قواعد الشركة الملزمة) تغطية كافية .

[1] - Jean Bacon and al (2018), op cit. n° 158.

يحظر قانون حماية البيانات المصري رقم ١٥١ لسنة ٢٠٢٠ إجراء عمليات نقل للبيانات الشخصية التي تم جمعها ، أو تجهيزها للمعالجة إلي دولة أجنبية ، أو تخزينها ، أو مشاركتها إلا بتوافر مستوي من الحماية لا يقل عن المستوي المنصوص عليه في هذا القانون.

[2] - Michele Fink op cit p.9-10.

وبما أن الموافقة الضمنية لا تكفي لعمليات النقل الدولية، فيجب أن تنص شروط استخدام المنصة على موافقة صريحة من المستخدم[١].

يجب أن تكون هناك حالات قليلة جدًا حيث يكون مراقب البيانات قادرًا على تبرير رفض تسليم المعلومات المطلوبة، حتى فيما يتعلق بطلبات نقل البيانات المتعددة. كما أن تكلفة بناء البنية التحتية للامتثال لهذه الطلبات لا علاقة لها بمفهوم الطلبات "المفرطة "وعلى وجه الخصوص" لا ينبغي تحميل التكاليف الإجمالية على أصحاب البيانات، ولا استخدامها ، لتبرير رفض الاستجابة لطلبات قابلية النقل"[٢] .

كما تؤكد اللائحة العامة لحماية البيانات على أن الحق في إمكانية نقل البيانات لا ينطبق إذا استطاع المراقب إثبات أنه ليس في وضع يسمح له بتحديد صاحب البيانات ما لم يقدم صاحب البيانات المزيد المعلومات لتمكين تحديد هويته[٣].

ترى اللجنة الوطنية لتكنولوجيا المعلومات والحريات الفرنسية(CNIL) أن تقنيات البلوك تشين لا تثير مشاكل تذكر عندما يتعلق الأمر بالامتثال لمتطلبات قابلية نقل البيانات ، حيث يمكن ممارسته بشكل فعال[٤].

[1] - Jean Bacon and al (2018), op cit. n° 159.
[2] - Groupe de travail Article 29 (5 avril 2017), op. cit 4 p.18
[3] - GDPR Art. 11(2)
[4] - Commission Nationale de l'Informatique et des Libertés (29 October 2018) Blockchain et RGPD : Solutions pour un usage responsable de la blockchain dans le cadre des données personnelles.

كما تؤكد اللائحة العامة لحماية البيانات على الاهتمام بتأمين قابلية التشغيل البيني بين البلوك تشين المختلفة.

يتعمق تقرير مرصد ومنتدى البلوك تشين في الاتحاد الأوروبي في مفهوم قابلية التشغيل البيني في سياق البلوك تشين ، ويعرّفه على أنه قدرة شبكات البلوك تشين المختلفة على التواصل ، وتبادل البيانات ، والرموز بشكل فعال.

تعتبر هذه القدرة محورية للتوسع والتطبيق العملي لتقنية البلوك تشين عبر مختلف القطاعات[١].

وقد تم التأكيد على ذلك فيما يتعلق بشبكات التواصل الاجتماعي حيث لا يكون هناك فائدة من نقل البيانات من مزود وسائط اجتماعية إلى آخر إذا لم يكن هناك "أصدقاء" في المزود الثاني[٢].

نفس المخاوف الناجمة عن تأثيرات الشبكة تنطبق أيضًا على سياق البلوك تشين ، سواء في البنية التحتية ، أو طبقات التطبيق ؛ وبالتالي فإن التنفيذ الفعال لقابلية نقل البيانات هو أحد الأسباب العديدة التي تدعو إلى تشجيع قابلية التشغيل البيني لمختلف الحلول.

---

https://www.cnil.fr/en/blockchain-and-gdpr-solutions-utilisation-responsable-blockchain-contexte-données-personnelles

[١] - لمزيد من المعلومات عن التقرير راجع : http://eublockchainforum.eu

[2] - Michele Fink op cit p.81.

المطلب الخامس

الحق في الاعتراض على معالجة البيانات الشخصية

يوفر الحق في الاعتراض إعادة تقييم فردية تعتمد على السياق لأغراض المعالجة ذات الصلة، وتحديدًا فيما يتعلق بالوضع الملموس لصاحب البيانات.

وفقًا للمادة ٢١ من اللائحة العامة لحماية البيانات يحق لصاحب البيانات الاعتراض ، لأسباب تتعلق بوضعه الخاص، في أي وقت ، على معالجة البيانات الشخصية المتعلقة به.

لن يقوم المراقب بمعالجة البيانات الشخصية ، ما لم يُظهر المراقب أسبابًا مشروعة مقنعة للمعالجة، والتي تتجاوز مصالح ، وحقوق ، وحريات صاحب البيانات ، أو لإنشاء المطالبات القانونية ، أو ممارستها ، أو الدفاع عنها.

يجب صياغة المصلحة بعبارات واضحة بما فيه الكفاية للسماح بتطبيق اختبار موازنتها مع مصلحة الشخص المعني وحقوقه الأساسية[1].

[1]- Groupe de travail Article 29 Sur La Protection Des Donnees Avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable dutraitement des données au sens de l'article 7 de la directive 95/46/CEAdopté le 9 avril 2014 p.27

يجب أن تكون المصالح المشروعة المقنعة المحتملة لمراقبي البيانات مفصلة ، ومعلنة ، ومتوقعة ؛ حتى يتمكنوا من تجاوز الرغبة الواضحة لأصحاب البيانات في إيقاف عملية المعالجة المعنية ؛ وذلك لأن المصالح المشروعة ليست بديلاً "سهلًا" للموافقة[١].

وقد أعرب مكتب مفوض المعلومات الأوربي عن قلقه من أن مراقبي البيانات على الإنترنت بشكل خاص، الذين يرون المصالح المشروعة على أنها "الخيار السهل" يفتقرون إلى "الفهم الكامل لما تتطلبه المصالح المشروعة[٢].

ونظرًا لأنه يُطلب من الأفراد صياغة وتقديم "أسباب" خاصة بحالتهم، والتي سيتم مقارنتها بأي أسباب مشروعة مقنعة لوحدة التحكم في البيانات، فيجب أن يتم تحديد المصلحة المشروعة لوحدة التحكم في البيانات مسبقًا.

عندما يمارس صاحب البيانات حقه في الاعتراض ، يجب على مراقب البيانات التوقف عن معالجة هذه البيانات الشخصية ما لم يكن في وضع يسمح له بإثبات "أسباب مشروعة مقنعة للمعالجة التي تتجاوز مصالح، وحقوق، وحريات صاحب البيانات، أو المؤسسة، أو لإنشاء المطالبات القانونية ،أو ممارستها ،أو الدفاع عنها[٣].

[1] - Jef Ausloos, Micheal Veale and René Mahieu, op cit n° 79
[2] - Information Commissioner's Office, 'Update Report into Adtech and Real Time Bidding' (20 June 2019) 18
[3] - GDPR, art 21(1)

تنطبق العديد من النقاط ذات الأهمية العامة الموضحة أعلاه أيضًا على الامتثال للمادة ٢١ من اللائحة العامة لحماية البيانات، مثل القدرة الفعلية لوحدات التحكم على التأثير على المعالجة ؛ بسبب وسائلها المحدودة للتدخل في البيانات، و أيضًا النقاط المتعلقة بالقدرة على إيقاف البيانات حيث تتم معالجتها تلقائيًا.

إحدى النقاط التي يتم التأكيد عليها بشكل خاص فيما يتعلق بالمادة ٢١ من اللائحة العامة لحماية البيانات ، هي التفسير الذي سيتم تقديمه "للأسباب المشروعة المقنعة" للمعالجة ؛ والتي تمكن مراقب البيانات من عدم إفساح المجال لطلب صاحب البيانات لممارسة حقه في تقييد المعالجة.

قد يتساءل المرء على عما إذا كانت مصلحة مراقب البيانات في سلامة سجلات DLT(دفتر الاستاذ الموزع) تكون مؤهلة على أنها مصلحة مشروعة ، وهذه مرة أخرى نقطة يمكن توضيحها من خلال التوجيهات التنظيمية لتوفير المزيد من اليقين القانوني في هذا المجال[١].

الواقع أن الحق في الاعتراض ليس له سوى نطاق تطبيق محدود ؛ لأنه ينطبق فقط على الحالات التي تعتمد فيها المعالجة على أحد السببين القانونيين الأخيرين في المادة ١/٦ ؛ لذلك ليس من المستغرب أنه منذ دخول اللائحة العامة لحماية البيانات

[1] - Michele Fink op cit p.82.

حيز التنفيذ ، تحول العديد من المراقبين الذين يعتمد نموذج أعمالهم بشكل كبير على التخصيص(والإعلان) ، من الاعتماد على الموافقة ، أو المصالح المشروعة[١] ، إلى الضرورة لأداء عقد [٢].

الاعتماد على هذا الأساس يجرد أصحاب البيانات بشكل فعال من القدرة على سحب موافقتهم[٣] ، أو الاعتراض على المعالجة المذكورة[٤].

في ضوء التوجيهات الاخيرة للمجلس الأوربي لحماية البيانات (EDPB) بشأن الأساس القانوني لضرورة العقد، قد يعتمد العديد من المراقبين بشكل غير قانوني على هذا الأساس[٥]، وسيكون من المفيد أن تحدد التوجيهات أن أصحاب البيانات لديهم الحق أيضًا – على نطاق أوسع – في الطعن في امتثال وحدات التحكم لأي من متطلبات اللائحة العامة لحماية البيانات حتى لو لم يكن ذلك مؤهلاً كحق ، على وجه الخصوص، يجب أن تحدد الإرشادات ما يجب أن يكون عليه التزام وحدة التحكم بالرد على مثل هذه المطالبات الخاصة بالمعالجة غير القانونية.

[1] - GDPR, art 6(1) a et f
[2] - GDPR, art 6(1) b
[3] - GDPR, art 7(4)
[4] - GDPR, art 21
[5] - Comité européen de la protection des données, « Lignes directrices 2/2019 sur le traitement des données personnelles en vertu de l'article 6, paragraphe 1, point b) du RGPD dans le contexte de la fourniture de services en ligne aux personnes concernées (version 2.0) » (8 octobre 2019)

المطلب السادس

الحق في تقييد معالجة البيانات الشخصية

تقييد المعالجة يعني وضع علامة على البيانات الشخصية المخزنة بهدف الحد من معالجتها في المستقبل.[١]

وفقًا للمادة ١٨ من اللائحة العامة لحماية البيانات يحق لصاحب البيانات تقييد المعالجة أثناء انتظار تقييم دقة أو فعالية الحق في الاعتراض، وكذلك في المواقف التي يدعي فيها أن المعالجة غير قانونية (لضمان الاحتفاظ بأدلة عدم المشروعية) وحيثما يرغب صاحب البيانات في التأكد من أن البيانات لا تزال موجودة لإنشاء المطالبات القانونية ، أو ممارستها ، أو الدفاع عنها.

إن الحق في تقييد المعالجة هو إجراء مؤقت، وبالنظر إلى الطريقة الآلية التي تعمل بها خدمات مجتمع المعلومات، فمن المهم تفعيل هذا الإجراء المؤقت ؛ لذلك يجب إعطاء الأولوية للحق في التقييد من حيث الوقت، وإخضاعه لإطار زمني أضيق بكثير من الحق في الاعتراض المرتبط به[٢].

[1] - GDPR, art 4(3).
[2] - Jef Ausloos, Micheal Veale and René Mahieu, op cit n° 86

توفر المادة ١٨ من اللائحة العامة لحماية البيانات الحق لصاحب البيانات في الحصول على تقييد لمعالجة البيانات الشخصية المتعلقة به في عدد من الظروف وبغض النظر عن التكنولوجيا المحددة المستخدمة لتنفيذ المعالجة.

نتيجة لذلك، حيثما تكون دفاتر الأستاذ الموزعة المستخدمة، يتطلب قانون حماية البيانات في الاتحاد الأوروبي أن يكون لدى صاحب البيانات إمكانية الحصول على تقييد للمعالجة، كما هو الحال عندما يطعن موضوع البيانات في دقة البيانات الشخصية.

من أجل تحديد ما إذا كان أحد وحدات التحكم المشتركة العديدة المحتملة في شبكة بلوك تشين معينة قادرًا على الامتثال لمتطلبات المادة ١٨ من القانون العام لحماية البيانات، يجب إجراء تحليل كل حالة على حدة للترتيبات الفنية والإدارية المحددة.

بشكل عام، يمكن وجود عقبات محتملة أمام الامتثال لهذا الالتزام ، فمن المحتمل أن تكون هناك عقبات فنية أمام تقييد المعالجة في سياقات المعالجة الآلية في تقنية البلوك تشين ؛ وذلك بسبب أنه غالبًا ما يتم تصميم هذه الأنظمة لجعل التدخل أحادي الجانب في معالجة البيانات أمرًا مرهقًا من أجل زيادة سلامة البيانات والثقة في الشبكة[١].

[1] - Michele Fink op cit p.79.

لا توجد وسيلة مباشرة لوقف معالجة البيانات الموجودة في إحدى الكتل، خاصة فيما يتعلق بالدفاتر العامة وغير المسموح بها.

كما أن هناك أيضًا تحديات تتعلق بالحوكمة فيما يتعلق بقدرة العديد من وحدات التحكم المشتركة المحتملة على القيام بمثل هذا التدخل في الشبكة.

لقد رأينا بشأن السيطرة المشتركة أن أي طرف يمارس درجة معينة من السيطرة على الوسائل ، وخاصة أغراض معالجة البيانات الشخصية مؤهل ليكون مراقبًا مشتركًا، ومع ذلك، فإن بعض وحدات التحكم في البيانات المحتملة مثل العُقد ، أو المستخدمين يفتقرون إلى القدرة على التدخل في الشبكة بطريقة من شأنها في الواقع أن تؤدي إلى تقييد المعالجة.

وهذا يؤكد مرة أخرى الأهمية المحورية لكل من الترتيبات الفنية والإدارية التي من شأنها تمكين مراقبي البيانات من الامتثال بشكل فعال للمادة ١٨ من اللائحة العامة لحماية البيانات.

تتطلب المادة ١٩ من اللائحة العامة لحماية البيانات أن يقوم مراقب البيانات بإبلاغ تصحيح البيانات الشخصية ، أو محوها، بالإضافة إلى أي قيود على المعالجة إلى "المستلمين" الذين تم الكشف عن البيانات الشخصية لهم.

وهذا يثير التساؤل حول ما هي الأطراف التي يمكن اعتبارهم "مستلمين" للبيانات الشخصية في السياقات التي يتم فيها استخدام تكنولوجيا البلوك تشين؟.

يتم تقديم تقنية البلوك تشين في كثير من الأحيان على أنها مفيدة للغاية حيث يتم استخدامها لتنسيق السجلات بين العديد من الأطراف المختلفة، مما يعني أنه من المحتمل أن يكون هناك على الأقل عدد كبير من هؤلاء "المستلمين" لكل عملية معالجة بيانات شخصية على دفتر الأستاذ الموزع.

في أنظمة البلوك تشين الخاصة يوجد عادةً سجل حافل للأطراف التي لديها إذن بالوصول إلى البيانات وقراءتها، مما يعني أن مراقبي البيانات يتتبعون البيانات الشخصية للأطراف التي يتم الكشف عنها ؛ ونتيجة لذلك، فإن الاتصال بهذه الأطراف لإبلاغهم بأي إجراءات بموجب المواد ١٦-١٨ من اللائحة العامة لحماية البيانات يجب أن يكون واضحًا نسبيًا.

على العكس من ذلك عندما تكون سلسلة الكتل عامة فلا حاجة إلى إذن للوصول إلى البيانات الشخصية المخزنة في هذه الدفاتر.؛ لأنه ليس لدى الأطراف المسؤولة عن هذه الشبكات أي طريقة لمعرفة الأطراف التي تمكنت من الوصول إليها من خلال البيانات الشخصية ذات الصلة، إما لأنها تعاملت بشكل مباشر مع الشبكة أو لأنها اعتمدت على أدوات مثل مستكشفي الكتل.

في هذه الظروف، يمكن القول أن واجبات الاتصال المتأصلة في المادة ١٩ من القانون العام لحماية البيانات "تستحيل" أو على الأقل "تتضمن جهدًا غير متناسب". نتيجة لذلك، قد يكون هذا أحد السيناريوهات المنصوص عليها في المادة ١٩ من اللائحة العامة لحماية البيانات حيث يحصل مراقب البيانات على إعفاء من الاضطرار إلى الامتثال لواجبات الإخطار الخاصة به[1].

[1] - Michele Fink op cit p.80.

خاتمة الدراسة

في ختام هذه الدراسة يمكن استخلاص النتائج التالية :

١–البلوك تشين عبارة عن قاعدة بيانات لا مركزية خالية من الوسطاء تجعل من الممكن أتمتة المعاملة ، والمصادقة عليها ، وختمها الزمني من خلال عُقد الشبكة، مع ضمان ثباتها ، وسرية البيانات من خلال التشفير غير المتماثل.

توفر تقنية البلوك تشين (سلاسل الكتل) حلاً لا مركزيًا يمكنه القضاء على نقاط الفشل الرئيسية في الأنظمة المركزية ، كما أن هذه التقنية تمثل حقبة جديدة في طريقة إنشاء الثقة بين فردين.

٢– تعتبر اللائحة الأوربية العامة لحماية البيانات(GDPR) إطارًا قانونيًا محايدًا من الناحية التكنولوجية، تم تصميمها بطريقة تتيح تطبيقها على أي تقنية ، حيث يقدم هذا التصميم العديد من المزايا، ليس أقلها أنه من المفترض أن يصمد أمام اختبار الزمن وأنه لا يميز بين تقنيات معينة ، أو حالات استخدامها.

٣– أبرزت هذه الدراسة أنه هناك توتر وعدم توافق كبير بين طبيعة تقنية البلوك تشين ، والهيكل العام اللائحة الأوربية العامة لحماية البيانات(GDPR).

ومن ناحية أخرى، فقد تم تسليط الضوء أيضًا على أن هذه الفئة من التقنيات يمكن أن تقدم مزايا قد تساعد في تحقيق بعض أهداف اللائحة العامة لحماية البيانات.

مع ذلك فقد تم التأكيد أيضًا على أن العلاقة بين التكنولوجيا والإطار القانوني لا يمكن تحديدها بطريقة عامة، بل يجب تحديدها على أساس كل حالة على حدة.

٤- إذا كان البلوك تشين غير متوافق إلى حد كبير مع العديد من المتطلبات التي حددتها اللائحة العامة لحماية البيانات ، ومع ذلك، فمن الممكن الاعتراض على اللائحة العامة لحماية البيانات (GDPR)، وربما حتى انتقادها، لتجاهلها تقنية مثل سلسلة الكتل (البلوك تشين).

٥- إن عدم توافق البلوك تشين العام مع اللائحة العامة لحماية البيانات ليس مطلقًا ؛ لأن هذه التكنولوجيا لا تزال حديثة ، يكتشف العالم تدريجيًا كيفية عملها ووظائفها.

وقد وجدت هذه الدراسة أنه لا يمكن الاستنتاج بطريقة عامة أن جميع سلاسل الكتل متوافقة أو غير متوافقة مع قانون حماية البيانات الأوروبي ، وبدلا من ذلك، يجب فحص كل استخدام للتكنولوجيا على أساس مزاياه الخاصة للوصول إلى مثل هذا الاستنتاج.

فإذا لم تكن تقنية البلوك تشين قادرة حاليًا على ضمان إخفاء الهوية الكاملة للمستخدم وحماية بياناته الشخصية بشكل فعال، فكم عدد اللاعبين الرقميين اليوم الذين يمكنهم التفاخر بهذا ؟ ربما ليس كثيرًا، إذا تابعنا عمليات سرقة البيانات العديدة التي تمت ملاحظتها على فيسبوك ، وغيره من التقنيات.

٦- إذا كان بإمكان البلوك تشين الخاص تنظيم نفسه ، وضمان امتثال معين للمتطلبات التنظيمية الثقيلة جدًا التي تفرضها اللائحة العامة لحماية البيانات (GDPR) بفضل طبيعته التعاقدية ، وحماية البيانات حسب التصميم. فالأمر مختلف بالنسبة للبلوك تشين العامة

ففي سلاسل الكتل الخاصة والمرخصة المشاركين معروفون للآخرين، مما يسمح بتعريف العلاقات التعاقدية التي تتيح التوزيع المناسب للمسؤولية.

علاوة على ذلك، فإن هذه الشبكات، على عكس الشبكات العامة وغير المسموح بها، مصممة بطريقة تتيح التحكم في الشبكة ، مما يجعل معالجة البيانات تتم بطريقة متوافقة، كما أن هناك سيطرة على الجهات الفاعلة التي يمكنها الوصول إلى البيانات الشخصية ذات الصلة، وهذا ليس هو الحال مع سلاسل الكتل العامة وغير المرخصة.

١١ - حماية البيانات الشخصية عبر تقنية البلوك تشين

٧- تعتمد اللائحة الأوربية العامة لحماية البيانات(GDPR)على الافتراض الأساسي بأنه فيما يتعلق بكل نقطة بيانات شخصية ، يوجد شخص طبيعي ، أو شخص اعتباري واحد على الأقل يكون مراقبا للبيانات، والذي يمكن لأصحاب البيانات مخاطبته لإنفاذ حقوقهم بموجب قانون حماية البيانات في الاتحاد الأوروبي.

مع ذلك، تسعى البلوك تشين في كثير من الأحيان إلى تحقيق اللامركزية في استبدال ممثل وحدوي بالعديد من اللاعبين المختلفين ، وهذا يجعل توزيع المسؤولية والمساءلة أمرًا مرهقًا، لا سيما في ضوء الخطوط الغامضة لمفهوم السيطرة (المشتركة) بموجب اللائحة العامة لحماية البيانات.

٨- تعطى اللائحة الأوربية العامة لحماية البيانات(GDPR) لصاحب البيانات حقوقا مطلقة وكثيرة على بياناته الشخصية – مما أدى إلى وصفها بأنها أصعب قانون للخصوصية والأمن في العالم – ، والمتمثلة في الحق في الحصول على المعلومات، حق الوصول للبيانات، الحق في تصحيح البيانات، الحق في محو البيانات، الحق في تقييد المعالجة، الحق في إمكانية نقل البيانات، الحق في الاعتراض على المعالجة ، والحقوق المتعلقة باتخاذ القرار الآلي.

مع ذلك فإن هذه الحقوق تتعارض في جوهرها مع نظام البلوك تشين غير القابل للتغيير.

حتى أنه على افتراض أنه يمكن تعديل البيانات ، أو محوها ، أو نقلها عند الضرورة للامتثال للمتطلبات القانونية ، ومع ذلك، فإن البلوك تشين تجعل مثل هذه التعديلات على البيانات مرهقة بشكل متعمد من أجل ضمان سلامة البيانات ، وزيادة الثقة في الشبكة.

٩- تولي اللائحة العامة لحماية البيانات أهمية كبيرة للاحتفاظ المحدود بالبيانات ، حيث يجب أن يكون الاحتفاظ بالبيانات الشخصية التي تتم معالجتها عند الحد الأدنى ، كما تكون معالجتها فقط للأغراض التي تم تحديدها مسبقًا ، ويجب حذفها عندما لا تعود ذات أهمية مباشرة للشخص الذي يحتفظ بها.

قد يكون من الصعب تطبيق هذه المبادئ على تقنيات البلوك تشين باعتبارها قواعد بيانات للإلحاق فقط وتنمو بشكل مستمر عند إضافة بيانات جديدة.

إضافة إلى ذلك، يتم نسخ هذه البيانات على العديد من أجهزة الكمبيوتر المختلفة. كلا الجانبين يمثلان مشكلة من منظور مبدأ تقليل البيانات.

علاوة على ذلك، ليس من الواضح كيف يجب تطبيق "الغرض" من معالجة البيانات الشخصية في سياق البلوك تشين ، وتحديدًا ما إذا كان هذا يشمل المعاملة الأولية فقط أو ما إذا كان يشمل أيضًا المعالجة المستمرة للبيانات الشخصية (مثل تخزينها واستخدامها لأغراض أخرى).

١١ - حماية البيانات الشخصية عبر تقنية البلوك تشين

١٠- أحد الحلول المقترحة في محاولة للتوفيق بين البلوك تشين ومتطلبات اللائحة العامة للبيانات بخصوص حقوق المستخدم على بياناته هو وجود نظامين متوازيين: البلوك تشين ، وقاعدة البيانات الكلاسيكية، وبهذه الطريقة، يمكن للبيانات الموجودة في قاعدة البيانات الكلاسيكية أن تلبي متطلبات اللائحة العامة لحماية البيانات.

مع كل معاملة جديدة، يتم إنشاء معرف المعاملة من أجل تحديد هذه المعاملة في نظام قاعدة البيانات. سيتم تخزين هذا المعرف على البلوك تشين ، مما يجعل من الممكن تأمين الوصول إلى البيانات، حيث أن المعرف خاص بحزمة البيانات. مما يضمن حصول المستخدم حقوق على بياناته الشخصية.

قائمة المراجع

المراجع باللغة العربية

١- أشرف جاد ، البلوك تشين والإثبات الرقمي في مجال حق المؤلف، المجلة الدولية للفقه والقضاء والتشريع ، العدد ١ ، ٢٠٢٠

٢- جهاد محمود عبد المبدي ، مدى حجية تقنية البلوك تشين في الإثبات المدني "دراسة تحليلية" المجلة الدولية للفقه و القضاء والتشريع المجلد ٤، العدد١ فبراير ٢٠٢٣

٣-خالد سويلم محمد سويلم ، الحماية القانونية للبيانات الشخصية الالكترونية ، دراسة مقارنة ، المجلة القانونية. مجلد . ١٤، العدد ٦ (٢٠٢٢)

٤- رحاب فايز أحمد سيد ، تقنية البلوك تشين وتوثيق الانتاج الفكري العربي ، مجلة المكتبات والمعلومات الرقمية ، س ٤٠، عدد ٢، ابريل ٢٠٢٠

٥- سعاد صالح أحمد أبوبكر، توجهات وتحديات تقنية البلوك تشين في حماية البيانات وضمان الخصوصية، المجلة الأفريقية للعلوم البحتة والتطبيقية المتقدمة (AJAPAS)، المجلد ٢، العدد ٣، يوليو–سبتمبر ٢٠٢٣.

٦- قميتى عفاف ، واقع وافاق استخدام تقنية البلوك تشين في اقتصاديات المنطقة العربية ، مجلة أبحاث اقتصادية معاصرة ، المجلد ٦، العدد ١ ، ٢٠٢٣.

٧-كافي زغير شنون ، الحماية القانونية للبيانات الشخصية الالكترونية ، مجلة الرافدين للحقوق ، المجلد ٢٣العدد ٨٤ السنة ٢٥- سبتمبر ٢٠٢٣.

٨- محمد أحمد المعداوي ، حماية الخصوصية المعلوماتية عبر مواقع التواصل الاجتماعي ، دراسة مقارنة ، مجلة كلية الشريعة والقانون بطنطا العدد ٣٣ الجزء الرابع ديسمبر ٢٠١٨

المراجع باللغة الفرنسية

Ouvrages speciaux et theses

1-Audrey Side, Benjamin MOLLET-VIEVILLE, et AugustinCordin, Master 2 Droit de la propriété intellectuelle appliquée Université Paris Est Créteil 2017-2018

2-Boris Barraud. Les blockchains et le droit. Revue Lamy Droit de l'immatériel, 2018.

3- Canter, Le conservatisme de la protection des données face à la révolution blockchain, in: cognitio 2019/1.

4- Cécile de Terwangne et Élise Degrave Avec la collaboration d'Antoine Delforge et de Loïck Gérard,La protection des données à caractère personnel en Belgique,Manuel de base, ISBN 978-2-509-03505-9 D/2019/8132/88

5- Cédric Strub , Contribution De La Blockchain Au Management Des Donnees De Sante , Memoire De Diplome D'État De Docteur En Pharmacie,Université de Strasbourg Faculté de Pharmacie,2020.

6-Claire Leveneur, Les Smart Contracts,Étude De Droit Des Contrats À L'Aune De La Blockchain.Thèse,Doctoral School of Private Law,Université Paris-Panthéon-Assas.2022.

7- Florence Chafiol, La blockchain à l'heure de l'entrée en application du règlement général sur la protection des données, Dalloz IP/IT 2017.

8- Hajar Moudoud,Intégration de la Blockchain à l'Internet des Objets.,these, Universite De Technologie De Troyes en Science Pour L'Ingenieur.2022.

9- Houiqua Ismail: Utilisation de Blockchain pour la sécurisation des données ERPs, diplôme de master académique Département d'informatique, Faculté des Sciences Exactes, des Sciences de la Nature et de la Vie, Algérie,2021/2022.

10- Jean-Marc Van GYSEGHEM et Cécile de Terwangne : « Analyse détaillée de la loi de protection des données et de son arrêté royal d'exécution », Vie privée et données à caractère personnel, Bruxelles, Politeia, 2013

11- Julien Rossi. Qu'est-ce que le droit à la protection des données à caractère personnel ?. Geopolitics of Risk Working Papers, 2018, Février . hal.

12- LE ROUX Corentin. Protection des données personnelles : Impact du RGPD sur les blockchains dans le secteur de la santé, Mémoire de MASTER 1 MIAGE, Université Paris 1 Panthéon – Sorbonne 2020/2021.

13-Poullet Y. et son équipe, «Rapport sur l'application des principes de protection des données aux réseaux mondiaux de télécommunications», Conseil de l'Europe, Comité consultatif T-PD, point 2.3.1, T-PD (2004) 04 final.

14- PRAZ EMILIE M., Responsabilités et outils de conformité selon la RGPD, PJA 2018

15- Sarah Sadik. La protection des données dans les contrats de cloud computing. these,. Université de Perpignan, 2023

16- Sébastien Drillon,La révolution Blockchain,La redéfinition des tiers de confiance,RTD Com. 2016.

17- Stéphane Bortzmeyer, La chaîne de blocs n’est pas immutable, 12 septembre 2016.

18- Thibault Douville,Blockchain et protection des données à caractère personnel, AJ contrat 2019

19- Thibaut Labbe,Le droit face aux technologies disruptives : le cas de la blockchain,These,Universite De Strasbourg ,École Doctorale ,2021.

20- Thibault Verblest ,Blockchain : une révolution juridique ?Revu Lamy Droit des Afferes N°129 SEPTEMBRE 2017

21- Vincent Gautrais, Les sept péchés de la blockchain : éloge du doute !Dalloz IP/IT 2019.

Rapports et équipes de travail

1-Commission de la protection de la Vie privée (CPVP), avis 26/2006 du 12 juillet 2006 concernant l’utilisation d’images satellites afin de dépister et de constater des infractions aux normes urbanistiques

2-Commission Nationale Informatique et Libertés (September 2018), Premiers Éléments d'analyse de la CNIL : Blockchain, 8-9.

3-Commission Nationale de l'Informatique et des Libertés (29 October 2018) Blockchain et RGPD : Solutions pour un usage responsable de la blockchain dans le cadre des données personnelles.

4-Commission Nationale de l'Informatique et des Libertés (06 November 2018) Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal datadata.

5- Groupe 29, Avis 4/2007 sur le concept de données à caractère personnel, p. 4 ; dans De Terwangne C. et Rosier K., Le Règlement général sur la protection des données (RGPD /GDPR), Analyse approfondie, 1re édition 2018, Larcier

6- Groupe 29, Sur La Protection Des Donnees-Avis 05/2012 sur l'informatique en nuage01037/12/FR.

7- Groupe 29, Sur La Protection Des Donnees Avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable dutraitement des données au sens de l'article 7 de la directive 95/46/CEAdopté le 9 avril 2014.

8- Groupe 29 (5 avril 2017), Lignes directrices sur le droit à la portabilité WP 16/EN, WP 242 rév.01, 4.

9- Les Impacts Dse Reseaux Distribues Et De La Technologie Blockchain Dans Les Activites De Marche Rapport Groupe Fintech Paris Europlace, 23 Octobre 2017

10-Rapport de la mission médiatique conjointe ,Informations sur la blockchain et ses usages (1) : L'enjeu de la souveraineté de décembre 2018.

المراجع باللغة الانجليزية

1- Guy Zyskind,Oz Nathan and Alex 'Sandy, Decentralizing Privacy: Using Blockchain to Protect Personal Data, 2015 IEEE Sec. & Privacy Workshops .

2-Information Commissioner's Office, 'Update Report into Adtech and Real Time Bidding' (20 June 2019)

3- Jef Ausloos, Micheal Veale and René Mahieu, Getting Data Subject Rights Right, 10 (2019) JIPITEC

4- Jean Bacon, Johan David Michels, Christopher Millard & Jatinder Singh, Blockchain Demystified: A Technical and Legal Introduction to Distributed and Centralised Ledgers, 25 Rich. J.L. & Tech., no. 1, 2018.

5- Kahina Khacef,Trade-Off Between Security And Scalability In Blockvhain Systems, Thesis, Doctoral School of Computer Science, Telecommunications and Electronics. Sorbonne University, 2022.

6- Michele Fink, Blockchains and Data Protection in the European Union, Max Planck Institute for Innovation and Competition Research Paper No. 18-01Juillet 2019

7- Mirko Koscina:Security and Optimization of Blockchains and Associated Algorithms,these, École doctorale Sciences Mathématiques de Paris Centre, Université Paris sciences et lettres 2021

8- Pavol Sokol, Jakub Mísek, and Martin Husák. „Honeypots and honeynets: issues of privacy“. In:EURASIP Journal on Information Security2017 (2017) pp. 1–9.

9- Powell, Kimberly. "French Surname Meanings and Origins." ThoughtCo, Aug. 29, 2020, thoughtco.com/french-surname-meanings-and-origins-1420788.

10-Supriya Adhatarao. On GDPR Compliant Data Processing. Cryptography and Security [cs.CR]. Université Grenoble Alpes [2020-..], 2021

11-Uk Government Office for Science ,A report by the UK Government Chief Scientific Adviser, Distributed Ledger Technology : beyond Block chain, 2016.h

المواقع الالكترونية

1- https://www.iab.com/wp-content/uploads/2019/10/IAB-HY19-Internet-Advertising-Revenue-Report.pdf
2- https://ec.europa.eu/digital-single-market/en/news/eprivacy-directive(cit. on p. 11.)
3- https://www.insee.fr/fr/accueil.
4- https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data
5- https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data
6- https://www.ethereum-france.com/la-chaine-de-blocs-nest-pas-immuable.
7- https://www.cnil.fr/sites/default/files/atoms/files/la_blockchain.pdf.
8- https://www.cnil.fr/en/blockchain-and-gdpr-solutions-utilisation-responsable-blockchain-contexte-données-personnelles
9- http://eublockchainforum.eu.