

Rapport thématique préparé par le European Union Blockchain Observatory & Forum

Catégorie de tensions	Extraits du rapport		Tension identifiée	Analyse contextuelle	Note d'interprétation				
	Extraits	Page et paragraphes			Lien avec la ventricule	Lien avec l'imaginaire sociotechnique	Acteurs impliqués	Recommandations	Comparaison internationale
Tension sur l'adoption de la numérisation des données personnelles	<p>To create a digital economy, we need to have similar kinds of growth, or "consistency" in the digital world. These two have been developed over the years, starting with simple digital representations of our physical, paper-based documents and moving on to more sophisticated means of digital identification like digital certificates, e-signatures, privacy-protocols like cryptography and hashing – methods that can help us uniquely identify a piece of digital data (for example a digital document) and "prove" ownership of it.</p>	Page 8, paragraphe 3	Les utilisateurs prennent la responsabilité complète de leurs données, augmentant les risques d'erreurs. Les titres qui étaient physiques avaient doncivement numériques. La fraude, le vol de documents officiels a toujours existé, mais ceux-ci sont mis en lumière avec les systèmes numériques	Les utilisateurs sont techniques peuvent mal gérer leurs identités, exposant leurs données ou perdant l'accès à leurs identifiants. Cela crée une fracture numérique car ceux qui ne possèdent pas les compétences nécessaires sont laissés pour compte dans l'adoption des systèmes numériques	Les concepts de solutions numériques font partie la technologie comme étant bénéfique, ignorant parfois les complexités liées à l'éducation et la capacité des utilisateurs à adopter ces nouvelles façons de fonctionner	L'imaginaire d'une souveraineté totale des utilisateurs est confronté à la réalité d'une expertise technique nécessaire, excluant les utilisateurs non formés ou vulnérables.	Developpeurs, gouvernements, utilisateurs/citoyens	Proposer des outils éducatifs et des interfaces simplifiées pour démocratiser l'accès à la digitalisation. Offrir des services d'accompagnement comme alternative temporaire aux utilisateurs novices.	L'Estonie a réussi à intégrer une identité numérique centralisée avec des interfaces conviviales, attirant une partie de sa population. L'interface utilisateur est devenue la plus utilisée, le hardware est une coquille à laquelle très peu veulent s'intéresser.
	<p>Another serious problem is that identity-related data is not secure. We have become accustomed to the fact that daily notices of data breaches revealing sensitive user data on mass to hackers and criminals, to the ease with which scammers can create fraudulent identities and use them to commit theft, including stealing identities from others, and to the complete lack of control we have over our personal data – data that we, knowingly or unknowingly, create when we are online, and which can be used to target or profit off us, even money on us, and potentially influence our</p>	Page 9, paragraphe 1							
Tension liée à la transparence des identités physiques à des identités numériques	<p>A typical use would be for a state to collect credentials from the government, for example that he or she is a citizen, or has a certain national ID number or lives at a certain address. When it comes time to make a choice, for example that he or she has the right to vote in an election or is old enough to purchase alcohol, the user can then simply present the appropriate credential.</p>	Page 13, paragraphe 4	Les utilisateurs doivent transporter leur identité dans le monde numérique. L'idée est de réaliser des identités décentralisées gérées par les citoyens mais garanties par les états et qui, augmente les risques de vulnérabilité.	Dans un système décentralisé, les données sont dispersées, ce qui rend les attaques de grande envergure plus complexes, mais les individus restent exposés à des erreurs de gestion, des pertes d'accès, des virus ou de la non connaissance d'urgence. Cette approche augmente également la dépendance à des fournisseurs de solutions de stockage sécurisé, ce qui pourrait centraliser à nouveau une partie du système.	Les entreprises vendant des solutions de gestion de données se positionnent comme indispensables, dévouant l'attention de la souveraineté individuelle. On fait parler le besoin de sécurité de données pour déléguer sa sécurité à un tiers.	L'imaginaire d'un contrôle total des utilisateurs sur leurs données est difficile par la nécessité de solutions techniques sécurisées qui ne peuvent être garanties que par des tiers.	Citoyens, fournisseurs de sécurité numérique	Encourager le développement de personnes de sécurité gouvernementale, accessible même aux dispositifs peu technologiques. Proposer des solutions open source pour réduire les dépendances.	Les États-Unis ont une approche complexe sur les projets de cybersecrétariat en confiant les données gouvernementales à des tiers de confiance mais ceux-ci investissent également dans des solutions open source.
	<p>Verifiable credentials play a key role in a decentralised identity framework. In essence, they are like digital versions of the physical credentials we carry around with us, such as our passports or driving licenses, though with additional properties made possible by their digital nature.</p>	Page 13, paragraphe 7							
Tension entre norme européenne et application nationale des normes	<p>The eIDAS regulation was born out of the Electronic Signatures Directive of 1999, which is a superseded. That directive, which was intended to provide a legal framework for the recognition of digital signatures across the European Union, was meant to facilitate cross-border electronic transactions through the use of electronic signatures throughout the Union.</p>	Page 19, paragraphe 8	Les gouvernements craignent une perte de contrôle sur les identités, ce qui pourrait affaiblir leur autorité dans des domaines tels que l'e-gouvernance, la fiscalité ou la sécurité nationale. Par ailleurs, les identités décentralisées augmentent le risque de création d'identités frauduleuses. La contre partie a été une perte de contrôle en un transfert au niveau européen de cette tâche sous une idée de gouvernance européenne.	Les gouvernements invoquent la sécurité nationale et la souveraineté pour limiter l'adoption du règlement sur l'identité numérique européenne.	L'imaginaire de liberté totale des utilisateurs dans un écosystème numérique décentralisé est confronté à la réalité des besoins de gouvernance et de contrôle étatique.	Gouvernements, agences de cybersecrétariat, union européenne	Combinaison des solutions centralisées et numériques serait une option pour garantir un pouvoir et une crédibilité étatique.	Promouvoir un projet d'identité européenne numérique devient une préoccupation majeure pour la continuité d'un pouvoir européen. Dépasser le cadre des états nationaux pour une adoption d'une identité européenne.	
	<p>Unfortunately, for various reasons – including the fact that, as a directive and not a regulation, it left decisions over implementation into local law in the hands of Member States, leading to a fractured, non-harmonised set of national approaches to its ambitions. As a binding regulation, eIDAS is mandatory for Member States and so will be applied uniformly.</p>	Page 20, paragraphe 1							
	<p>To implement this, eIDAS establishes a number of core principles binding on Member States, including the principle that Member States will cooperate on eIDAS and trust services and that citizens of one Member State can use their digital IDs obtained in one country in another country to get access to services across countries.</p>	Page 20, paragraphe 4							