Alors que tout ne monde ne parle que des plateformes numériques, la blockchain est l'anti-plateforme par excellence.

Brunessen Bertrand est professeur agrégé à l'Université Rennes 1, Chaire Jean Monnet sur la gouvernance des données (DataGouv) et responsable de l'Axe intégration européenne. Cet entretien a été publié le 19 mai 2022.

1/ Qu'apporte concrètement le nouveau Code de la Cybersécurité ?

Le Code de la cybersécurité a deux objectifs principaux.

Le premier, c'est la clarté du droit. Les questions de cybersécurité sont régies par une pluralité de textes français, européens et internationaux, dans une multitude de branches du droit. Cette dispersion actuelle des règles qui forment le droit de la cybersécurité rend la connaissance du droit de la cybersécurité difficile, ce qui est problématique à l'heure où ses enjeux deviennent considérables.

Cette fragmentation législative est liée au fait que les règles juridiques relatives aux questions de cybersécurité sont disséminées dans un grand nombre de textes : Code de la Sécurité intérieure, Code de la Défense, Code des Postes et des Communications Électroniques, Code pénal, Code de procédure pénale, les lois et règlements, directives européennes, etc. Cela crée un problème de sécurité juridique qui affaiblit la prévention et la réponse aux cyberattaques.

Le second, c'est l'intelligibilité et l'accessibilité du droit

pour toute personne, même non juriste, confrontée à des questions de cybersécurité. L'objectif du Code vise est de permettre à tout responsable de la prévention et de la réponse aux cyberattaques de trouver la réponse aux questions juridiques qu'il se pose.

C'est pour cela que le Code ne se limite pas à rassemble des textes épars, il propose aussi des commentaires de ces textes pour les expliquer et tenter de les rendre intelligibles pour ceux qui ne travaillent pas sur ces sujets. La pédagogie du droit est indispensable pour que chacun puisse se saisir de ces sujets.

2 / Quelle est la place du droit de l'Union européenne dans ce Code ?

Le Code de la cybersécurité rassemble les règles relatives aux trois couches matérielle (hardware), logicielle (software) et sémantique (la donnée). Pour cela, il rassemble plusieurs branches du droit qui peuvent être en pratique assez étanches.

D'une part, le droit de la sécurité des systèmes d'information, qui relève en France plutôt du droit privé. Ce sont les règles qui imposent aux entreprises la mise en place de mesures techniques et organisationnelles pour prévenir les cyberattaques et pour en atténuer les conséquences. D'autre part, le droit de la lutte contre la cybercriminalité, qui mobilise le droit pénal et la procédure pénale de droit français ainsi que des textes internationaux, on pense par exemple à la Convention de Budapest de 2001. Enfin, le droit de la cyberdéfense, qui relève davantage de règles de droit public, comme les règles relatives aux Opérateurs d'Importance Vitale (OIV).

Le droit de l'Union européenne cherche à réguler ces questions mais la compétence européenne n'est pas toujours évidente à déterminer, tant certains enjeux de sécurité restent régaliens.

Par exemple, la directive concernant la sécurité des réseaux et des systèmes d'information (NIS) est la première grande étape de la stratégie de cybersécurité proposée par la Commission en 2013. Son objectif principal, promouvoir la cyber-résilience dans l'UE, repose sur la nécessité de renforcer les capacités nationales et de développer une coopération entre les autorités publiques et le secteur privé. Pour sensibiliser les Etats (mais aussi les institutions européennes qui ont, pour certaines, pris peut être plus tardivement la mesure de ces enjeux), la Commission avait proposé une vision politique de la sécurité des réseaux et des systèmes d'information à travers plusieurs Communications (Communication sur la «Sécurité des réseaux et de l'information: proposition pour une approche politique européenne» en 2001, «Une stratégie pour une société de l'information sûre», de 2006, un Plan d'action et Communication sur la protection des infrastructures d'information critiques en 2009). L'enjeu de ces textes juridiquement non contraignants était de rassembler le consensus politique nécessaire autour de cette législation.

La question de la compétence de l'Union européenne pour agir sur ces questions est loin d'être évidente, mais les liens entre les Etats membres sont tels que les vulnérabilités de l'un d'entre eux peuvent avoir des effets systémiques au niveau européen. La directive NIS (en cours de révision) se fonde sur les mesures d'harmonisation nécessaires au bon fonctionnement du marché intérieur. Le prisme économique a été privilégié à un objectif de sécurité qui aurait soulevé de fortes contraintes juridiques pour justifier une action au niveau européen. La légitimité de l'action européenne est présentée à travers l'idée qu'une législation européenne, en permettant de faire face aux cyber-risques et menaces de dimension transnationale et en contribuant à une intervention coordonnée en cas d'urgence, doit favoriser le bon fonctionnement du marché intérieur (et accessoirement seulement accroître la sécurité intérieure de l'UE).

La directive NIS est cependant qu'une pièce de la législation européenne qui est elle-même très fragmentée : **pour avoir une idée générale du droit européen sur ces questions, il faut aussi se référer au Cybersécurity Act, au code européen des communications électroniques européen (directive de 2018), au règlement général sur la protection des données (RGPD), à la directive e-privacy**. A cela s'ajoute des législations sectorielles par exemple dans le domaine de la sûreté aérienne, de la sûreté de l'aviation civile, des services financiers, etc. Le règlement sur l'identification électronique et les services de confiance pour les transactions électroniques dans le marché intérieur (eIDAS) apporte des précisions importantes. Malgré cela, il reste encore quelques angles morts. La sécurité de l'internet des objets doit prochainement faire l'objet d'un Cyber Resilience Act. Ces enjeux rejoignent plus largement les questions d'autonomie stratégique européenne et la capacité de l'Union européenne à maîtriser ses chaines de valeurs industrielles.

3/ Comment expliquez-vous que la Blockchain soit encore aussi peu vulgarisée, et, cela va sans doute de pair, aussi peu prise au sérieux par le grand public ? La considérez-vous comme un élément incontournable de notre avenir ?

Je pense que cela tient essentiellement à deux choses : d'une part, à la difficulté du grand public à se représenter ce qu'est une blockchain. **Il y a un « coût d'entrée » pour en saisir pleinement les enjeux et comprendre le fonctionnement de cette technologie pour quelqu'un qui n'est pas spécialiste.** D'une part, cela tient sans doute au fait qu'elle reste encore associée de façon presque indissociables aux actifs numériques et que ses autres cas d'usage restent méconnus, en tout cas moins visibles.

Les applications de la blockchain (smarts contracts, traçabilité des chaines agroalimentaires ou dans l'industrie) laissent entrevoir des perspectives beaucoup plus larges si les éléments de fragilité de cette technologie parvenaient à

être renforcés : identité numérique, le transfert sécurisé de données, vote électronique, gouvernance des données de santé, les soins de santé, l'assurance, la finance, l'énergie, la logistique, la gestion des droits de propriété intellectuelle ou les services publics. Ces perspectives se heurtent encore à des questions de scalabilité et dépendent donc encore de la capacité de la recherche industrielle à permettre des utilisations de grande ampleur de cette technologie.

Les blockchains restent cependant opaques pour beaucoup et s'inscrivent un peu à rebours de l'intérêt du public pour les enjeux de régulation des grandes plateformes numériques. Alors que tout ne monde ne parle que des plateformes numériques, la blockchain est l'anti-plateforme par excellence.

La blockchain est en effet une technologie de stockage et de transmission d'informations permettant la constitution progressive d'un registre numérique dans lequel les données sont stockées et distribuées à l'ensemble des utilisateurs. Elle fait partie des DLT (distributed ledger technology) qui sont, plus largement, des registres distribués.

Les caractéristiques fondamentales de la blockchain sont ainsi la décentralisation et désintermédiation des transactions, l'immutabilité et l'irréversibilité et la transparence des données. Ces caractéristiques fondamentales, arrimées sur la technologie permettent d'envisager une sécurité accrue des échanges et des transactions au sein de ce registre. **C'est, fondamentalement, une infrastructure décentralisée : les données ne figurent pas dans un serveur central, elles sont transférées entre utilisateurs sans intermédiaire sur un réseau de pair à pair (peer to peer).**

C'est une technologie qui repose sur la décentralisation : en cela elle apparaît comme une technologie de rupture par comparaison avec les formes de centralisation du traitement et du stockage de donnée. Elle s'inscrit dans une logique de désintermédiation, par la suppression des tiers de confiance.

La décentralisation de son fonctionnement appelle des formes de gouvernance fondées, sous des modalités diverses, sur le consensus. Les enjeux économiques de la désintermédiation induite par cette technologie semblent fondamentaux. Ils sont présentés comme la nouvelle révolution de l'économie numérique.

C'est un registre distribué qui est tenu et partagé simultanément par tous les utilisateurs du réseau. Chaque donnée validée est copiée, le registre étant alors synchronisé et partagé entre les utilisateurs. Cette technologie repose sur un mode de gouvernance collective : les données sont enregistrées sur des blocs qui doivent être validés par les autres utilisateurs de ce registre. Chaque transaction doit être authentifiée et validée par les autres utilisateurs si elle répond aux règles de la blockchain. Ce registre se forme par des blocs successifs : d'où l'idée de chaine de blocs. Quand un bloc est validé, ses données sont partagées à tous les utilisateurs du registre et il ne peut plus être modifié. C'est là l'avantage et le problème de cette technologie pour la vie privée : les données validées dans la blockchain ne peuvent plus être modifiées.

La blockchain permet ainsi l'enregistrement successif des transactions par une technique d'horodatage. Ce fonctionnement garantit une forme de transparence, les transactions étant visibles par l'ensemble des utilisateurs, et une certaine irréversibilité : une donnée qui figure dans le registre ne peut plus être modifiée ou supprimée.

Ce mode de fonctionnement revendique des garanties d'authentification des transactions et d'intégrité des données (par l'horodatage et la traçabilité). La technologie de la blockchain soulève des questions de sécurité mais ses enjeux sont quelque peu différents des autres technologies car son protocole repose sur de la cryptographie qui le rendrait plus sécurisé. La constitution d'un bloc passe ainsi par un hachage des données. Chaque utilisateur dispose d'une clé publique et

une clé privée qui lui garantit une pseudonymisation pour ses transactions. **La sécurité est supposée être l'une des plus-values essentielle de la blockchain : la cryptographie rendrait les informations contenues dans ses registres infalsifiables. En outre, elle serait moins vulnérable aux cyberattaques qu'un système centralisé. Mais les risques de fraude ne sont pas écartés, au-delà même des questions récurrentes liées au blanchiment d'argent et au financement du terrorisme.**

Fondamentalement, la blockchain fait ainsi apparaître d'emblée quelques enjeux majeurs : le respect de la vie privée : comment appliquer le RGPD à une telle technologie ? et la dimension environnementale. Ces enjeux doivent pouvoir être maîtrisé pour un passage à l'échelle de cette technologie.

4/ Il est difficile de ne pas vous poser la question : en rigueur de termes, et du point de vue du droit constitutionnel, la souveraineté européenne, qu'elle soit politique, technologique ou numérique, existe-t-elle ou est-elle un "dahu" juridique destiné à servir une vision politique ?

Le thème de souveraineté européenne fait un retour inattendu dans le discours politique européen à la faveur d'une redéfinition de la politique européenne du numérique.

Plus que le numérique lui-même, c'est son ubiquité qui est, au fond, en cause, derrière l'idée de souveraineté : la souveraineté numérique concerne tout à la fois la politique de défense, la politique économique, la politique commerciale, la défense de la démocratie et des valeurs européennes, la régulation du marché intérieur, la cybersécurité.

Saisis dans leur intégralité, ces différents domaines qui, à leur façon, mettent en cause l'intégrité des compétences européennes et son autonomie, finissent par constituer quelque chose de fondamental et d'existentiel pour l'Union européenne

et ses États membres : son indépendance, sa capacité à garder la maîtrise de ses compétences les plus fondamentales et à appliquer les valeurs qui fondent sa raison d'être et son identité.

On comprend, dans ces conditions, ce dépassement d'une idée historiquement taboue pour montrer l'urgence d'une situation qui pourrait, à terme, en annihiler les enjeux.

À cela s'ajoute aussi la prise de conscience brutale, peut-être pour la première fois, des limites de chaque État face à ces enjeux. Si la rhétorique sur l'idée d'être plus forts ensemble cherche à cimenter une forme de solidarité européenne depuis toujours, la conscience, réelle, de la plus-value liée à l'appartenance au marché intérieur n'a jamais semblé non plus un horizon indépassable, comme l'a encore confirmé le Brexit.

Les avantages économiques ont toujours été soupesés à l'aune des contraintes politiques qu'implique l'appartenance à l'Union européenne et cette équation n'a rien d'une évidence dans un contexte de résurgence des populismes alimentés par l'envie de « reprendre le contrôle ». En ce qui concerne les enjeux de défense et de sécurité, la question n'a jamais pu être dissociée, par les États membres, de celle de la relation transatlantique et n'a donc jamais fait l'objet d'une approche européenne proprement autonome.

Pour la première fois, le numérique a créé une réelle rupture, par la prise de conscience, commune à tous les États membres, de leur incapacité individuelle à exister, défendre leurs valeurs, leur modèle, leur économie et leurs citoyens, seuls dans le cyberespace : la domination économique des plateformes américaines et chinoises, la puissance technologique des États-Unis et de la Chine ont révélé, sous un angle assez cruel, l'impuissance du soft power européen à exister et défendre ses choix, et ce constat est plus cinglant encore à l'échelle nationale. Face aux campagnes de désinformation et

de manipulation de l'opinion pour déstabiliser les démocraties européennes, aux cyberattaques des infrastructures sociales essentielles, à l'impuissance des économies à lutter contre la puissance de marché des plateformes, à la captation des données des citoyens et des industries européennes et à un retard technologique devenu évident, le sentiment d'impuissance individuelle des États membres semble avoir brisé le plafond de verre de la qualification des enjeux politiques qui se jouent désormais au niveau européen. **Si Paul-Henri Spaak a pu dire qu'il n'y avait « que deux types d'États en Europe : les petits… et ceux qui ne savent pas encore qu'ils le sont », le numérique a provoqué la prise de conscience des États appartenant à cette seconde catégorie.**

La conceptualisation de la souveraineté numérique européenne ne consiste pas à projeter la théorie de l'État au niveau européen, mais à penser l'indépendance, voire la mise en capacité d'agir, « l'empowerment », de la puissance publique européenne, dans une situation mondiale dans laquelle elle n'a pas su trouver sa place : rendre aux États européens une capacité d'agir dans un monde reconfiguré par le numérique. L'enjeu n'est donc pas la souveraineté européenne, ou alors une souveraineté inversée : une souveraineté numérique européenne qui rendrait aux États les moyens d'agir et leur indépendance. La mise en pouvoir d'agir des États membres dans le cyberespace passerait ainsi par l'Union européenne.

Les révélations d'Edward Snowden sur l'ampleur de la surveillance numérique de toutes les plus hautes autorités politiques européennes par les agences américaines, en particulier la NSA, et de la façon dont ces informations ont pu servir les intérêts américains ont sans doute créé une rupture dans l'inconscient européen, arrimé depuis toujours à une inaltérable alliance transatlantique. La stratégie de surveillance globale des principales puissances étrangères, aux fins de manipulations géostratégiques de l'Europe, est telle qu'elle ne peut pas ne pas affecter quelque peu au

passage la puissance de l'État et sa souveraineté-indépendance. À cela, s'ajoutent les stratégies de certaines puissances étrangères, plus spécifiquement la Chine et la Russie, qui ciblent les processus démocratiques des États par de multiples campagnes de désinformation et de manipulation des opinions publiques. Ajoutons la puissance économique des géants du numérique, dont le chiffre d'affaires approche parfois les recettes fiscales étatiques, et leur accumulation de grands volumes données, qui en font des acteurs qui tentent de jouer à jeu égal avec les États.

La fondamentalité et l'ubiquité de ces bouleversements ont fait prendre à l'Europe la mesure de son impuissance, si elle se limite à ne penser son action qu'à travers son marché intérieur. Même si ce marché intérieur reste au coeur de sa stratégie de reconquête numérique, par la création d'un espace européen des données ou la conditionnalité de l'accès aux données des citoyens au respect des règles européennes, l'aveu d'impuissance est là, et suscite un mouvement d'européanisation convergent.

D'un côté, les États acceptent l'européanisation des enjeux du numérique, – le Président français allant même jusqu'à évoquer la « souveraineté européenne » dans le domaine du numérique. Les États membres acceptent aussi, de fait, d'exercer en commun des compétences nationales, que la Commission coordonne avec des « boîtes à outils » (pour la 5G, pour l'e-santé, pour la numérisation de la justice) ou des « cadres » (pour le filtrage des investissements directs étrangers). Même les parlements nationaux, par essence attachés à la souveraineté nationale qu'ils représentent, en appellent à la souveraineté numérique européenne. Cette européanisation spontanée de questions relevant de compétences nationales est à mettre en lien avec l'importance des enjeux, en particulier la protection du modèle de démocratie libérale européenne, dès lors que les États européens sont désormais « dans une position de dépendance vis-à-vis des modèles américain du

capitalisme de surveillance et chinois du crédit social » ((selon les termes de la Proposition de résolution européenne du Sénat français du 21 oct. 2020 pour une localisation européenne des données personnelles). La marge de manoeuvre européenne est alors étroite : face à la structuration binaire entre États-Unis et Chine, dans laquelle la Russie cherche aussi à prendre sa part, l'Europe cherche encore sa place au niveau mondial, mais elle s'est imposée sur le plan interne comme le seul niveau d'action possible.

D'un autre côté, l'Europe assume aussi la nécessaire affirmation de son identité dans cette transformation numérique. **L'idée de souveraineté devient tangible et acquiert la force de l'évocation : elle s'affirme progressivement dans le discours politique, singulièrement dans le domaine numérique et, même si elle ne revêt pas la signification politico-juridique qu'elle implique, son apparition dans les discours, sans être de l'ordre du performatif, n'est pas neutre non plus, d'autant qu'elle s'accompagne de mesures très stratégiques, de la cybersécurité à la politique industrielle, en passant par la cyberdéfense, la régulation des plateformes ou la gouvernance des données. L'existence précède en quelque sorte l'essence** : la politique européenne du numérique existe et commence à porter ces enjeux fondamentaux, indépendamment de la façon dont on peut l'appréhender politiquement et juridiquement.

5/ Est-ce qu'il y a des visions différentes du juge français et du juge européen sur la question de la surveillance numérique ?

La question de l'accès des autorités publiques aux métadonnées de communications électroniques détenues par des opérateurs économiques cristallise aujourd'hui des débats juridiques et politiques fondamentaux. Au coeur des débats sur la révision de la directive et de la proposition de règlement e-privacy, elle fait parallèlement l'objet d'une jurisprudence fort audacieuse de la Cour de justice qui a choisi la question de

la protection des données personnelles, appliquée ici au droit des communications électroniques, pour défendre une jurisprudence volontariste et assez offensive, qui va bien au-delà des positions exprimées par les juridictions constitutionnelles nationales ou la CEDH. La jurisprudence européenne a ainsi ouvert ici une brèche qui commence à prendre des allures de bras de fer avec certaines juridictions nationales.

On sait, depuis l'arrêt Tele 2 rendu en 2016 par la Cour de justice de l'Union européenne, que les États membres ne peuvent imposer des obligations de conservation généralisée des données et que la gravité de l'ingérence dans les droits fondamentaux implique de ne réserver cette mesure qu'aux formes de criminalité les plus graves. Dès lors, dans une affaire « Quadrature du Net », la question s'est posée de savoir si la défense de la sécurité nationale justifiait quelques tempéraments à cette interdiction de toute conservation généralisée des données et d'accès à celles-ci. Sur ce point, le juge de l'Union européenne estime que, par nature, ces données permettent de tirer des conclusions très précises sur la vie privée des personnes. Ce raisonnement repose sur l'idée qu'il n'est pas possible d'apprécier concrètement la gravité de l'atteinte à la vie privée au moment de la demande d'accès.

Sans doute l'un des arrêts les plus attendus de ces dernières années, l'arrêt French Data Network rendu par le Conseil d'Etat le 21 avril 2021 a marqué une étape fondamentale sur ces questions de conservation et de l'accès des autorités publiques aux données de connexion. Sur le plan politique, il exprime la recherche d'un équilibre entre protection des données personnelles, vie privée et efficacité de la lutte contre la criminalité et le terrorisme et donc, au fond, une certaine vision de l'ordre politique et social. La sensibilité de ces enjeux est évidemment de nature à susciter de vives réactions dans la société.

Deux régimes législatifs français étaient contestés par les requérants au regard de la jurisprudence européenne : d'une part, l'obligation faite aux opérateurs de communications électroniques de conserver, pour une durée d'un an, de manière générale et indifférenciée les données de connexion pour la poursuite des infractions pénales, et, d'autre part, certaines techniques et missions des services de renseignement. Etait ainsi en cause le recours aux algorithmes par les services de renseignement, dans un contexte où un projet de loi relatif à la prévention d'actes de terrorisme et au renseignement cherche à pérenniser ce dispositif.

Pour la première fois depuis le début de la construction européenne, le gouvernement demandait au Conseil d'Etat de ne pas appliquer la jurisprudence de la Cour de justice de l'Union européenne afin de respecter plusieurs exigences constitutionnelles tenant au respect de la sauvegarde de la Nation, à la recherche des auteurs d'infractions pénales et à la lutte contre le terrorisme, dès lors que le recours aux données de connexion est devenu la principale technique d'investigation dans les enquêtes pénales et pour les services de renseignement.

Sur le plan juridique, l'enjeu était l'interprétation de la directive e-privacy par la Cour de justice qui, par une lecture très constructive du texte, avait condamné, dans un arrêt Tele 2, l'obligation de conservation généralisée des données de communications électroniques et la possibilité pour certaines autorités pénales d'y accéder. Précisons que sont essentiellement en cause les données de trafic et de localisation (et non le contenu des communications) comme les appels entrants et sortants, la durée des communications ou la localisation des appels.

La Cour de justice, estimant qu'il y a là une ingérence « particulièrement grave » dans la vie privée et la protection des données personnelles, interdit les législations nationales prévoyant une obligation de conservation générale et un accès,

même fortement conditionné, des autorités publiques à ces données pour la criminalité ordinaire. Précisant sa solution au fil des arrêts, elle a aussi décidé de limiter ces législations nationales à des mesures de conservation ciblées pour la lutte contre la criminalité la plus grave et les menaces contre la sécurité publique.

Dans l'arrêt French Data Network, le Conseil d'Etat propose une approche pragmatique. Pour ne pas écarter expressément le droit de l'Union, le juge trouve une solution dont le pragmatisme surprend : les données de connexion étant de toute façon conservées au titre de la sécurité nationale, la question de la conservation (ciblée ou non) ne se pose plus, en pratique pour les enquêtes pénales puisque, de fait, l'autorité judiciaire est en mesure d'accéder à ces données. Ainsi, « aussi longtemps que » les questions de sécurité nationale justifieront la conservation généralisée de ces données, la question de la conciliation entre le droit de l'Union et le droit constitutionnel ne se posera pas en pratique. La solution a le mérite de temporiser une situation, qui, de toute façon, est appelée à évoluer avec l'adoption proche du règlement e-privacy.

Ainsi, le Conseil d'Etat censure simplement les dispositions en tant qu'elles ne prévoient pas certaines garanties posées par la Cour de justice (réexamen périodique de la menace sur la sécurité nationale, avis de la commission nationale de contrôle des techniques de renseignement qui doit être contraignant) tout en laissant un délai au pouvoir réglementaire pour les intégrer aux textes.

Au passage, l'arrêt souligne les incohérences matérielles et conceptuelles de la solution de la Cour de justice : la conservation ciblée qu'elle prescrit s'avère impossible à appliquer dès lors qu'il n'est évidemment pas possible d'anticiper la commission d'un crime, ni de déterminer à l'avance où il se produira et encore moins de cibler, sans méconnaître le principe d'égalité, les individus susceptibles

de les commettre. **La conservation indifférenciée et généralisée, interdite par la Cour de justice, est pourtant nécessaire à l'efficacité des enquêtes pénales, donc au respect des exigences constitutionnelles de prévention des atteintes à l'ordre public et la sécurité des personnes et des biens, ainsi qu'à la recherche des auteurs d'infractions.**

Le bras de fer continue depuis, ponctué par des décisions du Conseil constitutionnel et de la Cour de justice en 2022.

On peut regretter que dans ces affaires, le raisonnement du juge ne distingue pas toujours suffisamment les enjeux entre la question de la conservation et celle de l'accès des autorités publiques à ces données. Or, pour accéder à des données, encore faut-il qu'elles soient au préalable conservées (de surcroît par des opérateurs privés, ce qui rend d'autant plus sensible la question de leur conservation). Ce serait alors surtout cette conservation généralisée qui serait attentatoire à la vie privée des citoyens, générant ce fameux sentiment, réel ou supposé, de « surveillance constante ». En pratique, on voit bien qu'il est difficile de réguler l'accès à ces données sans évoquer leur conservation. Une enquête pénale se déroule par définition après la commission d'infractions : si l'on autorise dans certains cas, en l'occurrence pour la criminalité la plus grave, l'accès à ces données, cela présuppose nécessairement qu'elles ont toutes été conservées puisqu'il n'est pas possible d'anticiper la commission de telles infractions et de cibler par avance la conservation de ces données. Admettre des hypothèses d'accès, même restreint, à ces données n'implique-t-il pas une conservation générale ? Dans ces conditions, **il apparaît nécessaire de sécuriser davantage la conservation de ces données (tant sur le plan technique que juridique). Ainsi, la question de l'accès pourrait être régulée pour elle-même, sans être appréhendée à travers les inquiétudes, distinctes, que soulève la question de leur conservation.**

6/ Treize membres de l'UE s'opposent à l'idée d'une réforme

des traités dans le but "d'aller plus vite" en renonçant à l'unanimité des voix sur certaines questions. L'Union au forceps, n'est-ce pas la promesse de sécessions futures ?

C'est un débat éternel dans l'Union européenne, qui a fait l'objet de révisions régulières des traités et de compromis politique, comme le compromis de Luxembourg en 1966 suite à la politique de la « chaise vide » conduite par la France.

C'est au cœur de la méthode européenne : une stratégie des petits pas, qui permet de progresser mais lentement, et par étapes. **Toute l'histoire de la construction politique européenne repose sur un élargissement constant du vote à la majorité qualifiée.** Ainsi, d'une certaine façon, la proposition d'une réforme des traités sur ce point s'inscrit dans le sens de l'histoire.

Elle se justifie aussi, sans doute, par un moment très particulier pour l'Union européenne confrontée à une montée des populismes en son sein et à une revendication des « démocraties illibérales ». Très concrètement, la situation de la Pologne et de la Hongrie posent des questions sur le fonctionnement des institutions puisque leur stratégie est souvent de faire cause commune pour bloquer les décisions. Cette stratégie de blocage peut résulter de leur opposition directe sur un texte, mais peut être aussi un jeu à plusieurs bandes, pour obtenir des arbitrages favorables sur d'autres textes. L'extension du vote à la majorité qualifiée limiterait ces stratégies, en retirant aux Etats membre le droit de veto que leur confère en pratique l'unanimité.

Ce n'est qu'une proposition qui devra de toute façon recueillir l'unanimité des Etats membres (ainsi qu'une ratification de chaque Etat selon ses règles constitutionnelles internes) pour permettre une modification des traités. Si les Etats membres consentent à ces évolutions, ce n'est pas en fonction d'une vision irénique qu'ils se font de la construction européenne mais c'est parce qu'ils y

trouvent un intérêt. En outre, il n'y a (théoriquement) rien d'irréversible : ce que les Etats ont fait, ils peuvent de la même façon le défaire.

Je soulignerais deux tempéraments à la réaction provoquée par cette proposition.

D'une part, la pratique politique est beaucoup plus souple que les règles de vote ne le laissent entendre, ce qui atténue en pratique la distinction unanimité/majorité qualifiée. La pratique politique est celle de la discussion et du consensus au sein du Conseil. Il est même souvent arrivé qu'il n'y ait pas de vote formel, tant les discussions en amont avaient permis de réunir un consensus politique sur un texte. Je mets à part certains domaines très singuliers, comme la politique étrangère et de sécurité commune qui fonctionne selon un mode de gouvernance très différent : elle reste très intergouvernementale en tout état de cause.

D'autre part, les malentendus sur le sens de la construction européenne, avec des conséquences comme le Brexit, sont en effet fondamentaux, mais je ne suis pas sure qu'ils résultent des modalités de vote. Je pense que la clarification fondamentale à opérer porte sur le sens de la construction européenne, ce que l'on a toujours évité de faire. Que veut-on faire de l'Union européenne ? Une construction politique avec une identité propre, commune ? Ou un marché intérieur qui donne des avantages économiques à ceux qui y participent ? Tant que l'on maintiendra l'ambiguïté sur cette question fondamentale, qui ne tranche pas l'opposition qui existe entre des conceptions opposées du projet européen, on se heurtera à ces divergences.