Droit Public Comparé
ISSN : 3036-2490

2 | 2024

L'influence des nouvelles technologies sur l'action de l'Union européenne en matière de sécurité publique

Mouna Mouncif-Moungache

https://publications-prairial.fr/droit-public-compare/index.php?id=444

DOI : 10.35562/droit-public-compare.444

Electronic reference
Mouna Mouncif-Moungache, « L'influence des nouvelles technologies sur l'action de l'Union européenne en matière de sécurité publique », *Droit Public Comparé* [Online], 2 | 2024, Online since 02 juillet 2024, connection on 03 juillet 2024.
URL : https://publications-prairial.fr/droit-public-compare/index.php?id=444

L'influence des nouvelles technologies sur l'action de l'Union européenne en matière de sécurité publique

Mouna Mouncif-Moungache

OUTLINE

TEXT

> « [L]'État n'a pas pour fin de transformer les hommes d'êtres raisonnables en animaux ou en automates, mais bien de faire en sorte que les citoyens développent en sécurité leur corps et leur esprit, fassent librement usage de leur raison, ne rivalisent point entre eux de haine, de fureur et de ruse, et ne se considèrent point d'un œil jaloux et injuste. La fin de l'État, c'est donc véritablement la liberté[1]. »

1 À l'instar de ce qu'ont pu décrire des visionnaires ou des spécialistes de science-fiction, la tentation de surveiller massivement grâce aux technologies numériques, afin de prévenir tout risque pour la sécurité des biens et des personnes, n'est pas l'apanage d'États non démocratiques. Chacun aura pu constater la facilité, liée à une certaine nécessité, avec laquelle le numérique s'est imposé dans le domaine de la sécurité sanitaire attestant la thèse d'un biopouvoir[2]. Si l'équilibre entre sécurité et liberté est forcément difficile à atteindre, force est de constater que les évènements liés au terrorisme ou à la pandémie, et peut-être bientôt au changement climatique, rendent les débats complexes. La sécurité dépend de l'espace géographique dans lequel il se construit, mais aussi de son espace-temps. Des phénomènes nouveaux apparaissent et l'autorité publique doit réagir de manière adéquate. À l'échelle d'un État, la sécurité occupe une place prépondérante si nous en voulons pour preuve le contrat social qui en fait un fondement essentiel de la naissance d'un État. L'État est devenu l'acteur principal de la sécurité des individus au nom d'un contrat social[3]. Cette sécurisation passe donc par celle de l'État. Mais les États ne sont pas les seuls à être préoccupés par la nécessaire sécurité. Dans sa communication relative à la stratégie de l'Union européenne en matière de sécurité, la Commission européenne rappelle, à juste titre, que la

responsabilité première de la sécurité appartient aux États membres. Pour autant, les évolutions quant à l'importance et l'étendue des menaces pour la sécurité ont pour conséquence un besoin et une volonté de l'Union européenne de jouer un rôle en matière de sécurité. Dans ses orientations politiques, la Commission a indiqué clairement qu'il ne fallait négliger aucun aspect pour protéger les citoyens. La cybercriminalité ou encore le terrorisme sont autant des dangers soulignés par la Commission européenne dans sa communication sur l'union de la sécurité, présentée le 24 juillet 2020 [4]. Elle préconise à cet égard la mise en place d'un « solide écosystème européen de la sécurité » fondé sur la recherche et l'innovation dans ce domaine.

2 La notion de sécurité n'est pas en soi facile à définir. Elle est présente dans les constitutions de plusieurs États, sans pour autant qu'une définition positive de celle-ci soit fournie. Le sens qui lui est donné varie en fonction des différentes traditions juridiques nationales et s'articule, « tantôt comme un droit subjectif des individus à l'intégrité physique, tantôt comme une des missions régaliennes de l'État [5] ». La sécurité a pu être qualifiée de droit fondamental et comme l'une des conditions de l'exercice des libertés individuelles et collectives [6]. La « sûreté » mentionnée par l'article 2 de la Déclaration des droits de l'homme et du citoyen comme étant un « droit naturel et imprescriptible de l'homme » est une garantie contre les abus du pouvoir.

3 La sécurité publique, quant à elle, est une composante de la sécurité *lato sensu*. Associée à l'ordre public sans se confondre à ce dernier, la sécurité publique est un outil de prévention, de surveillance et plus globalement de police administrative. À ce titre, les nouvelles technologies permettent la surveillance généralisée et de masse. L'usage des drones [7] et des caméras de surveillance avec outils d'analyse en est un bel exemple. La protection de la sécurité publique est aussi un pan du droit pénal étant entendu que la frontière entre la prévention et la répression n'est pas toujours aisée. La frontière est devenue d'autant plus poreuse que l'on constate que les menaces ont évolué contribuant ainsi à une gestion plus globale de la sécurité. « La répression pénale…participe à la sécurité publique [8] ». Cette porosité est encore plus prégnante lorsqu'elle étudie la manière dont l'Union européenne s'investit dans ces champs. En effet, les mesures prises

par l'Union européenne intégrant les nouvelles technologies impliquent une approche globale de la question de la sécurité sans pour autant les confondre. Il s'agit non seulement de lutter contre la criminalité, mais également de la prévenir. L'usage des nouvelles technologies permet d'agir de manière efficace sur les deux pans, ce qui influence de manière importante la manière dont les États membres protègent la sécurité publique. L'Union européenne a acquis une compétence en matière de sécurité au fur et à mesure de la construction européenne, ce qui, en matière de nouvelles technologies, crée des tensions importantes entre l'Union européenne et les États comme en atteste l'adoption du règlement sur l'intelligence artificielle [9] sur lequel nous reviendrons dans les développements ultérieurs.

4 Dans un premier temps, la sécurité publique a exclusivement permis aux États membres de préserver, voire de créer, des mesures contraires aux libertés de circulation [10], sous réserve d'une interprétation de l'exception par application du principe de proportionnalité. À cet égard, il convient de noter que la marge d'appréciation des États membres s'est réduite. Il a été justement relevé que la sécurité publique fait l'objet d'un encadrement plus poussé [11] dans le cadre de l'interprétation des restrictions qui peuvent être apportées à une liberté en l'occurrence la libre circulation des marchandises. Dans un second temps, l'Union européenne agit indirectement en matière de sécurité publique grâce à la compétence qu'elle détient au titre de l'espace de liberté, de sécurité et de justice [12] et en matière de technologies numériques. Depuis le début des années quatre-vingt-dix, d'importantes initiatives sont prises, dont la création d'un « espace de liberté, de sécurité et de justice » par le traité d'Amsterdam. Le contrôle aux frontières ou encore la lutte contre l'immigration illégale, ou le maintien de l'ordre deviennent des enjeux d'intervention de l'Union européenne. Elle devient un acteur de la sécurité intérieure des États membres en définissant des priorités et en modifiant les systèmes juridiques en vigueur [13]. Le titre V du traité sur le fonctionnement de l'Union européenne consacré à l'espace de liberté, de sécurité et de justice contient un article 67 [14] qui en précise les objectifs. Outre des dispositions générales, ce titre contient un chapitre spécifique, consacré à chacun des domaines que sont les politiques relatives aux

contrôles aux frontières, à l'asile et à l'immigration, coopération judiciaire en matière civile, coopération judiciaire en matière pénale et coopération policière. La disparition des piliers a conduit à un mouvement d'intégration des questions relevant de la sécurité contribuant à marquer un peu plus les possibilités d'action de l'Union européenne en la matière. En sus de cette évolution, l'Union européenne dispose également d'un nouveau levier d'intervention grâce à la réglementation qu'elle adopte dans le domaine des technologies numériques. Une Union européenne armée pour faire face aux évolutions des technologies numériques [15] pourrait résumer la perspective dans laquelle elle s'inscrit. Ce mouvement initié depuis quelques années connaît une forte accélération depuis 2020. La Commission européenne a présenté le 9 mars 2021 une communication sur la décennie numérique de l'Europe : « 2030 digital compass : the European way for the digital decade » qui présente les grands objectifs de la politique numérique européenne d'ici à 2030. Favoriser l'émergence d'un secteur du numérique français et européen fort est un enjeu de sécurité. Dans son mouvement d'engrenage permanent, l'Union européenne continue à approfondir son action en matière de sécurité. Ce mouvement devient encore plus patent lorsque l'Union européenne, à l'instar de l'ensemble des États, considère que les nouvelles technologies sont simultanément un potentiel et un danger qu'il convient de maîtriser pour assurer la sécurité publique. L'Union européenne est une puissance normative qu'elle met au service des nouvelles technologies et de la sécurité publique. Compte tenu des dangers que cela représente pour les droits fondamentaux, l'Union européenne s'est attachée par ses institutions et organes à trouver un équilibre, afin que les nouvelles technologies numériques utilisées dans le domaine de la sécurité publique ne soient liberticides. L'objectif consiste donc à traiter certains points saillants et d'actualité du sujet [16]. L'Union européenne s'appuie sur les technologies numériques pour assurer la sécurité publique. Par conséquent, l'usage des technologies numériques en matière de sécurité publique positionne l'Union européenne comme autre acteur de celle-ci (1.). Cette nouvelle configuration conduit l'Union européenne à s'affirmer en même temps comme défenseur des droits fondamentaux (2.).

1. L'usage des technologies numériques positionne l'Union européenne comme un autre acteur de la sécurité publique

5 Bien qu'étant les principaux acteurs de la sécurité publique, les États n'en ont plus le monopole absolu. Les évolutions de la construction européenne expliquent que l'action des États membres en matière de sécurité publique voit ses contours partiellement redessinés. L'adoption simultanée d'un corps de règles dans le domaine de la sécurité et en matière de technologies numériques positionne l'Union européenne comme un acteur stratégique de la sécurité, et *in fine* de la sécurité publique. Alors que les initiatives de l'Union européenne s'appuient sur les nouvelles technologies pour redynamiser les dispositifs de coopération entre États membres (1.1.), les normes juridiques ayant pour objet l'usage les nouvelles technologies contribuent à encadrer l'action des États membres en matière de sécurité publique (1.2.).

1.1 L'Union européenne redynamise la coopération entre États membres

6 Les dangers pour la sécurité sont transnationaux. Ils ont accru et ont changé de nature. Les États membres doivent offrir une approche, *a minima*, coordonnée afin de répondre de manière satisfaisante à ces nouveaux enjeux, dans l'objectif de protéger au mieux la sécurité publique. Si la compétence nationale reste de principe pour assurer la sécurité de chaque territoire, le but est d'intensifier les coopérations au bénéfice d'une plus grande sécurité de chacun. En vertu du principe de subsidiarité, l'Union européenne se définit comme étant la mieux placée pour répondre à ces défis. Conformément à l'article 4, paragraphe 2, point j) du TFUE, la compétence pour adopter des mesures dans le domaine de la liberté, de la sécurité et de la justice est partagée entre l'Union européenne et ses États membres. Les États membres ne peuvent donc agir seuls pour réglementer l'utilisation des canaux de communication numériques. Sans action

de l'Union européenne, les progrès sont plus lents et il est par définition plus difficile d'assurer l'interopérabilité des canaux de communication au niveau de l'Union. Les fondements juridiques issus des traités ont permis la création de plusieurs organes et objectifs [17] qui s'appuient sur les technologies numériques et l'échange de données pour accélérer le processus et le rendre plus efficace.

7 Europol et le système d'information Schengen sont des exemples topiques de ce qui peut être entrepris et de l'influence des nouvelles technologies. Europol est un office créé par acte du Conseil du 26 juillet 1995 qui coordonne, organise et réalise des enquêtes et des actions opérationnelles pour soutenir et renforcer les actions des autorités compétentes des États membres. Il soutient les activités d'échange d'informations pour lutter essentiellement contre les infractions pénales. Bien qu'Europol soit pensé pour mener des enquêtes policières dans le cadre d'enquêtes pénales, son champ d'action a des implications sur la manière dont les États peuvent assurer la sécurité publique. En effet, le centre opérationnel coordonne l'aide qu'Europol peut apporter au maintien de l'ordre lors des grandes manifestations, c'est-à-dire les rassemblements culturels, politiques, économiques ou sportifs de premier plan au niveau international qui représentent une cible ou une occasion pour la criminalité et le terrorisme. Le niveau de coopération a été amélioré en modernisant les instruments disponibles [18]. Lors des sessions de mai et juin 2022, dans le cadre de la procédure législative ordinaire, les députés du Parlement européen [19] ont approuvé un accord conclu en février par les négociateurs du Parlement européen et du Conseil visant à donner à Europol plus de pouvoir. La réforme établit des règles claires et une base juridique pour le traitement des données volumineuses et complexes afin d'améliorer le partage d'informations, l'utilisation de l'intelligence artificielle ou la prise de décision par algorithmique. La possibilité qui lui est donnée de fournir aux États membres des renseignements et une aide à l'analyse lorsqu'ont lieu des manifestations internationales importantes n'est pas négligeable du point de vue des missions confiées à l'État même si cela reste marginal. Certes, les États membres demeurent selon les traités [20], responsables du maintien de l'ordre public et de la sauvegarde de la sécurité nationale, pour autant la mission confiée à

Europol a des implications quant au maintien d'ordre public et de la sécurité publique.

8 Le système d'information Schengen est une autre illustration de la manière dont les nouvelles technologies peuvent faire évoluer la prise en charge de la sécurité publique par les États membres. Ce système d'information a été instauré afin d'assurer un niveau élevé de sécurité dans l'espace de liberté, de sécurité et de justice de l'Union européenne, y compris la préservation de la sécurité publique et de l'ordre public et la sauvegarde de la sécurité sur les territoires des États membres. La gestion des frontières est devenue un lieu privilégié de l'utilisation des nouvelles technologies. Les frontières seraient devenues, elles aussi, *intelligentes*. Ainsi, le système d'entrée et de sortie de l'espace Schengen a créé une base de données commune qui enregistre les informations sur les ressortissants de pays tiers, telles que le nom, le document de voyage, les empreintes digitales, la photo faciale, la date et le lieu d'entrée, de sortie ou de refus d'entrée dans l'espace Schengen. Il s'agit d'un système électronique qui stocke les données non seulement des voyageurs soumis à l'obligation de visa, mais aussi de ceux qui en sont exemptés et admis à séjourner jusqu'à 90 jours. Ces données sont mises à disposition d'Europol. À cet égard, dans le cadre de son nouveau mandat, Europol a la possibilité de proposer aux États membres l'introduction de signalements reçus de pays hors Union européenne ou d'organisations internationales dans le système d'information Schengen II [21] (SIS II) qui a pour objet de permettre aux États membres de l'espace Schengen de mettre en place une politique commune de contrôle des entrées dans l'espace Schengen et, ainsi, de faciliter la libre circulation de leurs ressortissants tout en préservant l'ordre et la sécurité publics [22]. Ces informations se présenteraient sous la forme d'alertes et seraient uniquement accessibles aux policiers situés dans la zone Schengen et aux frontières extérieures de l'Union européenne. Ainsi, l'article 10 du règlement dispose que « [l]orsqu'un État membre a pris une décision de retour, conformément à l'article 6, paragraphe 2, de la directive 2008/115/CE, et envisage d'introduire un signalement concernant le retour au sujet d'un ressortissant de pays tiers qui est titulaire d'un titre de séjour ou d'un visa de long séjour en cours de validité, octroyé par un autre État membre, les États membres

concernés se consultent par la voie d'échange d'informations supplémentaires, et notamment lorsqu'il prend la décision en question, l'État membre d'octroi tient compte des motifs de la décision de l'État membre qui a pris la décision de retour et il prend en considération, conformément au droit national, toute menace pour l'ordre public ou la sécurité publique que pourrait représenter la présence du ressortissant de pays tiers en question sur le territoire des États membres. En vertu du règlement 2018/1862 qui étend l'utilisation du SIS en faveur de la coopération entre les autorités policière et judiciaire, le signalement et l'échange d'informations et de données couvrent également les contrôles ayant pour objet la prévention contre les menaces pour la sécurité publique. Ces différents dispositifs ont ainsi fait dire à la doctrine que « [l]e recours à des fichiers et systèmes informatiques de plus perfectionnés consacre le passage de la frontière juridique la frontière électronique [23] ».

9 Les initiatives prises par l'Union européenne tendent à vouloir encadrer l'usage des nouvelles technologies dans le domaine de la sécurité publique au sein des États membres.

1.2. L'Union européenne tente de cadrer l'action des États membres

10 Les professionnels de la prévention et de la répression de chacun des États membres doivent s'adapter aux nouvelles technologies en acquérant de nouvelles compétences et en intégrant de nouvelles techniques d'enquêtes et de surveillance. Les normes juridiques adoptées par le droit de l'Union européenne en matière de nouvelles technologies notamment sur le fondement de la compétence qu'elle détient au titre du marché intérieur ont des répercussions directes sur la manière dont les États membres pourront faire usage de ces nouvelles technologies pour assurer la sécurité publique dans l'espace physique et l'espace virtuel sur leur territoire. Deux cas concrets peuvent être présentés. L'utilisation de l'intelligence artificielle pour la surveillance de l'espace public et la cybersécurité sont deux exemples pour lesquels l'encadrement des nouvelles technologies redessine partiellement l'usage qui peut en être fait par les États en matière de sécurité publique.

11 L'intelligence artificielle [24] est une technologie en pleine expansion dont les conséquences ne sont pas toutes connues. En tout état de cause, elle constitue assurément un outil puissant de lutte contre la criminalité et de surveillance grâce à l'analyse de grandes quantités d'informations. L'analyse extrêmement rapide informations issues des réseaux sociaux, de la géolocalisation, des sons, des vidéos permet d'orienter les forces de sécurité contribuant ainsi non seulement à détecter des infractions, mais même à la prévoir. Plus généralement, il s'agit d'un outil de surveillance de plus en plus performant. L'analyse prédictive ne consiste pas bien entendu à notre capacité à lire dans l'avenir, mais à se fonder sur des données agrégées qui reflètent une situation à un instant donné. Nous retrouvons ainsi le débat majeur de l'analyse *prédictive* [25] de tous les actes mettant en jeu la sécurité [26]. La proposition de règlement relatif à l'intelligence artificielle (en voie d'adoption définitive [27]) est un texte très général et fondé en particulier, mais non exclusivement, sur le fonctionnement du marché intérieur [28]. Il prévoit l'utilisation de cette technologie notamment en tentant d'encadrer les possibilités d'une surveillance de grande ampleur justifiée pour des raisons de sécurité. De manière générale, il est important de constater que le règlement entend contraindre le plus possible les autorités nationales tout en tenant compte des exigences des États quant à la nécessité de préserver la spécificité du champ de la sécurité [29]. Ainsi, la classification de système d'IA de surveillance dans la catégorie de systèmes interdits a un impact sur la manière dont les États membres doivent pouvoir y recourir. Si le principe est l'interdiction de l'utilisation des systèmes d'identification biométrique à distance « en temps réel [30] » dans des espaces accessibles au public à des fins répressives, le règlement précise les cas où cette surveillance est autorisée. On retrouve plusieurs éléments qui attestent de cette volonté d'encadrer. L'utilisation de cette technologie n'est possible que, dans certains cas, comme la prévention d'une menace spécifique, substantielle et imminente pour la vie ou la sécurité physique des personnes physiques ou la prévention de menaces réelles, actuelles ou prévisibles comme c'est le cas pour les attentats terroristes. Il s'agit d'autoriser cette utilisation de manière exceptionnelle et strictement nécessaire. Par conséquent, le texte prévoit que l'utilisation doit tenir compte d'un certain nombre d'éléments tels la nature de la situation notamment sa gravité ou l'ampleur du préjudicie potentiel, mais aussi

les conséquences de l'utilisation sur les droits et libertés. Cela revient bien entendu à l'appréciation des États membres qui devront prévoir une procédure d'autorisation administrative ou judiciaire. En outre, il convient de préciser que d'autres dispositifs d'exemption ont été négociés. Si les fournisseurs et organismes publics qui entendent utiliser des systèmes d'IA à haut risque doivent les déclarer dans une base de données, les services de police et de contrôle des migrations pourront bénéficier d'un dispositif particulier non public. Enfin, l'évaluation de la conformité est écartée dans des situations exceptionnelles, puisqu'une procédure d'urgence a été introduite afin de permettre aux services répressifs compétents d'utiliser et déployer un outil d'intelligence artificielle répertorié selon les critères du règlement comme « à haut risque » sans passer par la procédure d'évaluation de la conformité [31]. Cependant, l'Union européenne entend cadrer cette possibilité en précisant que « l'autorisation visée au paragraphe 1 n'est délivrée que si l'autorité de surveillance du marché conclut que le système d'IA à haut risque satisfait aux exigences du chapitre 2 du présent titre. L'autorité de surveillance du marché informe la Commission et les autres États membres de toute autorisation délivrée conformément au paragraphe 1. Cette obligation ne couvre pas les données opérationnelles sensibles relatives aux activités des autorités répressives ».

12 Il convient de noter que le Comité européen de la protection des données avait demandé que la reconnaissance faciale soit interdite dans les lieux publics au sein de l'Union européenne. Fin 2021, les eurodéputés avaient également adopté un moratoire sur l'utilisation de la reconnaissance faciale par la police. Cette résolution avait été adoptée par le Parlement européen [32] qui réclamait la définition d'un cadre juridique précis.

13 L'espace numérique est aussi l'objet de nombreuses attaques qui peuvent mettre en danger la sécurité publique faisant de ce nouvel espace le lieu de la création d'un ordre public numérique [33]. Les nouvelles technologies constituent un atout du point de vue de l'Union européenne afin de prévenir et lutter contre la criminalité dans l'espace virtuel. La cybercriminalité est un concept très large qui englobe tous les dangers en matière de sécurité publique que l'on peut connaître dans ce nouvel espace qu'est le numérique. La

cybercriminalité est nouvelle catégorie d'infractions [34] dont s'est emparée l'Union européenne. Elle s'appuie sur plusieurs types de dispositifs et de nombreux textes à l'image du caractère protéiforme de cette notion. Le Conseil et le Parlement européen se sont mis d'accord sur des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, afin d'améliorer encore la résilience et les capacités de réaction aux incidents du secteur public comme du secteur privé et de l'Union européenne dans son ensemble. Le 13 mai 2022, le Conseil et le Parlement européen sur le fondement de l'article 114 du TFUE ont trouvé un nouvel accord sur le contenu de la nouvelle directive dite « SRI 2 [35] » qui remplace l'actuelle directive [36] sur la sécurité des réseaux et des systèmes d'information afin de supprimer les divergences entre États membres. L'obligation d'identifier les opérateurs de services essentiels a donné lieu à une évaluation globale qui montre les progrès encore à faire en la matière [37]. En effet, ont été constatés le faible niveau de prise de conscience conjointe de la situation et l'absence de réponse conjointe à la crise. Par exemple, dans un État membre, certains grands hôpitaux ne relèvent pas du champ d'application de la directive SRI et ne sont donc pas tenus de mettre en œuvre les mesures de sécurité qui en découlent, tandis que dans un autre État membre, la quasi-totalité des fournisseurs de soins de santé du pays est couverte par les exigences en matière de sécurité des réseaux et des systèmes d'information. Elle a pour objet la définition des mesures de gestion des risques en matière de cybersécurité et des obligations en matière de signalement dans tous les secteurs couverts par la directive. Si la directive s'attache à respecter les compétences des États membres en matière de sécurité publique, il n'en demeure pas moins qu'elle a un impact notable sur la conception même de sécurité publique qui implique la sécurité des réseaux des structures publiques et privées. La directive précise qu'elle serait « sans préjudice des compétences des États membres concernant la préservation de la sécurité publique, de la défense et de la sécurité nationale [38] » et que les États membres ne seraient pas tenus, dans le cadre des mécanismes d'échanges d'informations, de « fournir des renseignements dont la divulgation serait contraire aux intérêts essentiels de [leur] sécurité intérieure » (considérant 6). Bien que le texte précise également que la directive ne s'appliquera pas aux entités exerçant des activités dans

des domaines tels que la défense ou la sécurité nationale, la sécurité publique, les services répressifs et le pouvoir judiciaire, il n'en demeure pas moins que les actions entreprises en la matière ont un impact sur la manière dont la sécurité publique est protégée. En effet, il est indiqué que la nouvelle directive s'appliquera aux entités de l'administration publique aux niveaux central et régional. En outre, les États membres peuvent décider de l'appliquer également à ce type d'entités au niveau local. À ce titre, les États membres sont dans l'obligation d'identifier des opérateurs de services essentiels et d'imposer aux opérateurs des mesures de gestion des risques pour la sécurité des réseaux. Cette obligation qui s'impose aux États contribue à envisager la question de la sécurité publique sous un nouvel angle avec une vision élargie des dangers et des acteurs indirects de la sécurité publique. Les entreprises et les entités publiques sont ainsi pleinement impliquées dans la mise en place de protocole de gestion des risques sur les réseaux numériques.

14 Si l'usage des technologies numériques constitue une avancée importante pour assurer la sécurité publique, il s'agit d'un danger majeur pour les droits fondamentaux dont l'Union européenne doit assurer la protection, car la confiance ne se décrète pas. Celle-ci doit être le résultat d'une véritable stratégie de contrôle des usages des nouvelles technologies en conformité aux droits fondamentaux.

2. L'usage des nouvelles technologies positionne l'Union européenne comme protectrice des droits fondamentaux

15 L'Union européenne doit veiller également à ce que l'usage des nouvelles technologies en matière de sécurité publique reste fondé sur les valeurs européennes communes, à savoir le respect de l'État de droit, de l'égalité et des droits fondamentaux. La sécurité et le respect des droits fondamentaux ne sauraient être envisagés comme des objectifs contradictoires. En particulier dans une Union de droit. S'appuyant sur un corpus juridique, cette stratégie de l'Union européenne est délimitée par un contrôle *administratif* et

juridictionnel. Le contrôle juridictionnel est assuré en partie par la Cour de justice qui rend une interprétation délimitant l'action des États (2.1.). Le contrôle exercé par des autorités indépendantes permet de la réguler (2.2.).

2.1. L'action des États délimitée par l'interprétation rendue par la Cour de justice

16 Afin d'éviter que les technologies numériques ne soient des « outils d'asservissement [39] », les ordres juridiques pour lesquels la protection des droits fondamentaux constitue une valeur importante, telles que l'Union européenne, se doivent de dessiner un système suffisamment robuste. On note ainsi une vigilance de l'Union européenne qui se manifeste dans le contenu des normes adoptées par les institutions de l'UE notamment dans le cadre du RGPD et surtout de la directive du 27 avril 2016 [40], mais aussi par des interprétations des textes par la Cour de justice saisie sur renvoi préjudiciel. Dans tous les cas, la recherche de l'équilibre n'est pas simple en particulier lorsqu'on apprécie le potentiel de ces nouvelles technologies pour la sécurité publique et pour l'innovation sujet sur lequel l'Union européenne souhaite fortement se positionner. Le rapport de la Commission européenne, relatif à l'application de la Charte des droits fondamentaux pour l'année 2021, a souligné la nécessité d'une « stratégie visant à renforcer l'application de la Charte des droits fondamentaux dans l'Union européenne [41] ». Elle a ainsi prévu de travailler en partenariat avec les autres institutions et agences de l'Union européenne, dont l'Agence des droits fondamentaux. Le rapport montre comment la situation évolue dans les États membres, et comment ces derniers et la Commission européenne ont recours à la Charte pour surmonter les différents obstacles. Parmi tous les sujets qui peuvent être abordés se trouve la question de l'utilisation des données personnelles par les autorités étatiques. La Cour de justice a élaboré une jurisprudence de plus en plus centrale permettant de rappeler l'importance et la nécessité d'une protection des données personnelles, en particulier dans le champ de la sécurité publique. Toute personne dans l'Union européenne, dont les données à caractère personnel font l'objet d'un

traitement, est protégée par le cadre juridique adopté par l'Union européenne conformément à l'article 8 de la Charte et à l'article 16 du Traité sur le fonctionnement de l'Union européenne. L'enjeu en matière de sécurité publique est de trouver le bon équilibre, comme l'a souligné le Parlement européen dès la conception des politiques en matière de sécurité [42]. En effet, en vertu de l'article 52 de la Charte, les droits des personnes peuvent être restreints dans des circonstances très spécifiques, uniquement si cela est nécessaire et proportionné, dans une société démocratique, pour répondre effectivement à des objectifs d'intérêt général expressément reconnus par la législation de l'Union européenne en matière de protection des données. Les arrêts rendus par la Cour de justice de l'Union européenne en la matière soulignent le fait que l'Union européenne se positionne comme un espace juridique protecteur des données personnelles [43] et font apparaître les points de tension avec les États membres quant à leur volonté de préserver leur marge d'action en matière de sécurité publique.

17 La jurisprudence de la Cour permet de déterminer le cadre des obligations qui s'imposent aux États membres lorsqu'ils se saisissent des données pour protéger la sécurité publique. Dans les affaires sur lesquelles elle a eu à statuer, la Cour de justice s'est prononcée sur l'interprétation de l'article 15 §1 de la directive du 25 novembre 2009 [44] qui prévoit une exception à l'interdiction de conserver des données sans le consentement de la personne concernée. Comme la doctrine l'a justement relevé, la Cour a condamné le stockage de masse des données à caractère personnel, « de façon généralisée et indifférenciée [45] ». Le champ d'application de la directive protégeant les communications électroniques est large. Pour autant, celle-ci entend prendre en considération la particularité du champ de la sécurité. Ainsi, « une conservation généralisée et indifférenciée des métadonnées à d'autres fins telles que la prévention, la recherche, la détection ou la poursuite d'infractions pénales n'est pas conforme au droit de l'Union européenne dans la mesure où l'objectif n'est pas suffisamment grave pour justifier une telle ingérence dans les droits et libertés fondamentaux [46] ». S'agissant de l'accès des autorités nationales compétentes aux données conservées, la Cour confirme que la réglementation nationale concernée ne saurait se limiter à

exiger que l'accès réponde à l'un des objectifs visés à la directive. Elle doit également prévoir les conditions matérielles et procédurales régissant l'accès des autorités nationales compétentes aux données conservées. Cette réglementation doit se fonder sur des critères objectifs pour définir les circonstances et les conditions dans lesquelles l'accès aux données doit être accordé aux autorités nationales compétentes, étant entendu que la défense de la sécurité publique est prise en compte par la Cour comme situation particulière. Cette dernière précise d'ailleurs les obligations des États membres à qui il appartient d'instaurer un contrôle préalable effectué par une juridiction ou une entité indépendante et d'en informer les personnes concernées.

18 Les conditions de conservation des données dépendent de la manière dont on qualifie la sécurité. Dans l'affaire du 5 avril 2022, la Cour tient à la distinction qu'il n'est pas aisé d'opérer entre sécurité nationale et sécurité publique, ce qui a été justement relevé par la doctrine [47]. Cette distinction est fondamentale en ce que seule la nécessité de protéger la sécurité nationale peut permettre à l'État de conserver de manière généralisée et indifférenciée les données. La Cour de justice considère que les données relatives au trafic et des données de localisation ne pourraient être conservées de manière justifiée autrement que par la nécessité de sauvegarder la sécurité nationale qui « dépasse celle des autres objectifs visés à l'article 15, paragraphe 1, de la directive 2002/58 ». Dans ce cas (sécurité nationale), la Cour a jugé que l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, « ne s'oppose pas, en principe, à *une mesure législative qui autorise les autorités compétentes à enjoindre* aux fournisseurs de services de communications électroniques de procéder à la *conservation* des données relatives au trafic et des données de localisation de l'ensemble des utilisateurs des moyens de communications électroniques *pendant une période limitée*, dès lors qu'il existe des circonstances suffisamment concrètes permettant de considérer que l'État membre concerné fait face à une menace grave [...] pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible [48] ». Les États membres font le choix d'une conception large de la sécurité nationale [49]. La Cour de justice permet de donner

des indications sur l'utilisation des données en cas de menace grave pour la sécurité publique en listant différentes hypothèses. Sont ainsi compatibles avec la directive

> « une conservation ciblée des données relatives au trafic et des données de localisation qui soit délimitée, sur la base d'éléments objectifs et non discriminatoires, en fonction de catégories de personnes concernées ou au moyen d'un critère géographique, pour une période temporellement limitée au strict nécessaire, mais renouvelable ; une conservation généralisée et indifférenciée des adresses IP attribuées à la source d'une connexion, pour une période temporellement limitée au strict nécessaire ; une conservation généralisée et indifférenciée des données relatives à l'identité civile des utilisateurs de moyens de communications électroniques, et le recours à une injonction faite aux fournisseurs de services de communications électroniques, au moyen d'une décision de l'autorité compétente soumise à un contrôle juridictionnel effectif, de procéder, pour une durée déterminée, à la conservation rapide des données relatives au trafic et des données de localisation dont disposent ces fournisseurs de services, dès lors que ces mesures assurent, par des règles claires et précises, que la conservation des données en cause est subordonnée au respect des conditions matérielles et procédurales y afférentes et que les personnes concernées disposent de garanties effectives contre les risques d'abus [50] ».

19 Plus récemment la Cour de Justice de l'Union européenne saisie d'une question préjudicielle relative notamment à l'interprétation de l'article 5 de la directive 2016/680 [51], a considéré que

> « celui-ci s'oppose à une législation nationale qui prévoit la conservation, par les autorités de police, à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, de données à caractère personnel, notamment de données biométriques et génétiques, concernant des personnes ayant fait l'objet d'une condamnation pénale définitive pour une infraction pénale intentionnelle relevant de l'action publique, et ce jusqu'au décès de la personne concernée, y compris en cas de réhabilitation de celle-ci, sans mettre à la charge du responsable du traitement l'obligation de vérifier régulièrement si cette conservation est toujours nécessaire,

> ni reconnaître à ladite personne le droit à l'effacement de ces données, dès lors que leur conservation n'est plus nécessaire au regard des finalités pour lesquelles elles ont été traitées, ou, le cas échéant, à la limitation du traitement de celles-ci [52] ».

20 Les différents arrêts rendus par la Cour montrent les nombreux points de friction entre entre des intérêts divergents. Cette jurisprudence sera sans doute de plus en plus abondante dans les années à venir avec en parallèle une interprétation de la Cour européenne des droits de l'homme qui sera aussi saisie de ce type de questions et qui sera sans doute prise en considération par la Cour de justice de l'Union européenne.

21 La jurisprudence de la Cour de justice est complétée par l'action des agences européennes qui, par le contrôle qu'elles exercent, assurent un rôle de régulateur.

2.2. L'action des États régulée par le contrôle les autorités européennes indépendantes

22 Si un contrôle politique est exercé par les institutions de l'Union européenne notamment par le Parlement européen lors du processus décisionnel ou par le truchement de l'adoption de résolutions [53], un contrôle plus expert et plus indépendant est aussi exercé par les agences de l'Union européenne [54], ce qui contribue à renforcer la protection des droits. Ce contrôle s'exerce *a priori* et *a posteriori*. À ce titre, deux autorités jouent un rôle important, mais non exclusif d'autres autorités. Elles jouent un rôle *a priori* en exerçant une activité de conseil auprès des institutions de l'Union européenne et des États. Elles interviennent de ce fait dans le processus décisionnel contribuant à en renforcer la *crédibilité* par le degré d'expertise qu'elles apportent. Elles exercent également des missions *a posteriori* en contrôlant l'application des règles. Il convient de noter à titre subsidiaire que des autorités nationales ont été désignées par les États membres afin de protéger les individus et en particulier leurs données (ex. la CNIL en France). On peut donc souvent identifier un double dispositif de coopération entre les États membres et l'échelon

européen ainsi qu'une coopération entre les agences européennes elles-mêmes.

23 Ainsi, l'Agence européenne des droits fondamentaux, instituée en 2007 [55] a pour mission de fournir aux institutions et autorités compétentes de l'Union et des États membres, lorsqu'ils mettent en œuvre le droit de l'Union européenne, des informations, une assistance et des compétences en matière de droits fondamentaux. Par conséquent, elle a en charge la collecte, le recensement, l'analyse et la diffusion des informations en matière de droits fondamentaux. En revanche, son action reste limitée dans la mesure où elle ne peut prendre des décisions. Elle mène ses actions notamment en coopération avec le contrôleur européen de la protection des données (CEPD), l'Agence de l'Union européenne, chargée de la sécurité des réseaux et de l'information (ENISA) et le Centre commun de recherche (JRC) de la Commission européenne, et de manière à compléter leur travail. L'Agence européenne a poursuivi son travail de promotion des droits fondamentaux dans l'utilisation des technologies numériques. Son rapport de 2018 sur l'utilisation des données biométriques dans les systèmes d'information à grande échelle a révélé des insuffisances d'information aux personnes lors de la prise d'empreintes digitales à des fins d'immigration, d'asile et de gestion des frontières. Afin d'améliorer l'information aux migrants et aux demandeurs d'asile enregistrés dans la base de données dactyloscopiques européenne en matière d'asile (Eurodac) [56], l'agence a publié une brochure conjointement avec le Groupe de coordination du contrôle d'Eurodac en janvier 2020. Il s'agit d'accompagner les autorités à délivrer une meilleure information aux citoyens sur les raisons pour lesquelles les empreintes digitales sont prises et sur ce qu'il advient des données biométriques stockées dans Eurodac.

24 Le CEPD (Comité européen de la protection des données), quant à lui, exerce plusieurs fonctions et a des missions importantes dont le périmètre s'est élargi avec le RGPD. En vertu de l'article 43 du RGPD, le rôle de conseiller indépendant que joue le CEPD auprès des institutions de l'Union européenne couvre tous les aspects du traitement de données à caractère personnel, notamment les initiatives visant à renforcer la sécurité dans l'Union européenne et les nouveaux outils d'échange de données utilisés par les services répressifs. Le système d'information sur les visas, contentant des

données à caractère personnel sur les demandeurs de visa, est supervisé par les autorités de contrôle nationales et le contrôleur européen de la protection des données du système d'information sur les visas. En effet, le rôle du CEPD ne consiste plus uniquement en la surveillance et la garantie de l'applicabilité des dispositions du règlement du 11 mai 2016, mais également des dispositions du règlement (UE) 2018/1725 [57] . Il exerce donc un contrôle sur les institutions et organes de l'Union européenne garantissant de ce fait le respect de la protection des données personnelles.

25 Les possibilités offertes par les nouvelles technologies pour assurer la sécurité publique sont nettes et révèlent tout leur potentiel. Bien qu'étant cadrées par la nécessaire protection des droits fondamentaux, elles font apparaître les difficultés à trouver un équilibre satisfaisant entre la protection de la sécurité publique d'une part et la protection des droits fondamentaux d'autre part. Ressurgit dans ce nouveau contexte technologique le débat sur l'existence d'un droit fondamental à la sécurité [58] ayant conduit à considérer, en matière de sécurité sanitaire, que désormais la sécurité était au-dessus des lois comme l'affirmait Michel Foucault. Cette période marquée par des ruptures et des effondrements structurels (tels qu'en matière d'environnement ou de santé) est particulièrement propice à faire ressurgir une demande accrue de sécurité de la part des États, voire de celle des individus.

NOTES

1 B. Spinoza, *Traité théologico-politique* [1670], E. Saisset (trad.), Saint-Martin-de-Londres, H&O éditions, 2018, p. 176.

2 M. Foucault, *Naissance de la biopolitique : cours au collège de France, 1978-1979*, Paris, Gallimard-Seuil, coll. « Hautes études », 2004.

3 J.-J. Rousseau, *Du contrat social* [1762], Paris, F. Rieder, 1922.

4 Commission européenne, *Communication au Parlement européen, au Conseil européen, au Conseil, au Comité économique et social européen et au Comité des Régions relative à la stratégie de l'UE pour l'union de la sécurité*, Bruxelles, le 24 juillet 2020, COM (2020) 605 final.

5 F. Natoli, « Sécurité et ordre public : deux notions à relations variables. Comparaison franco-italienne », *Revue des droits de l'homme*, 2017, nº 11, DOI : 10.4000/revdh.2905.

6 *Loc. cit.*

7 M. Bouchet, « Les drones face aux enjeux de droit pénal et de libertés fondamentales », *Dalloz IP/IT : droit de la propriété intellectuelle et du numérique*, Paris, Dalloz, 2022, p. 299-303.

8 F. Lamy, « La production de la sécurité publique », dans *Ordre public et libertés publiques*, colloque organisé par l'Association française de philosophie du droit, 17 et 18 septembre 2015,URL : https://www.conseil-etat.fr/publications-colloques/discours-et-interventions/ordre-public-et-libertes-publiques .

9 Commission européenne, *Proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle et modifiant certains actes législatifs de l'Union*, SEC (2021) final, Buxelles, 21 avril 2021, COM (2021), 206 final. La proposition après plusieurs modifications a été adoptée définitivement par le Parlement européen le 13 mars 2024 et par le Conseil en avril de la même année.

10 M. Blanquet, « L'appropriation par la Communauté européenne des impératifs de sécurité », *in* : *Qu'en est-il de la sécurité des personnes et des biens*, Toulouse, Presses universitaires de l'université de Toulouse 1 Capitole, LGDJ, 2006, p. 175.

11 F. Picod, « Libertés de circulation des marchandises », *JurisClasseur*, synthèse, septembre 2023.

12 G. Giudicelli-Delage. et C. Lazerges, *Le droit pénal de l'Union européenne au lendemain du Traité de Lisbonne*, Paris, Société de législation comparée, coll. « Unité mixte de recherche de droit comparé », vol. 28, 2012

13 D. Zerouki-Cottin, « L'espace pénal européen : A la croisée des chemins ? », *Revue de droit pénal et de criminologie*, 2013.

14 « L'Union constitue un espace de liberté, de sécurité et de justice dans le respect des droits fondamentaux et des différents systèmes et traditions juridiques des États membres. […] Elle assure l'absence de contrôles des personnes aux frontières intérieures et développe une politique commune en matière d'asile, d'immigration et de contrôle des frontières extérieures qui est fondée sur la solidarité entre États membres et qui est équitable à l'égard des ressortissants des pays tiers. Aux fins du présent titre, les

apatrides sont assimilés aux ressortissants des pays tiers. […] L'Union œuvre pour assurer un niveau élevé de sécurité par des mesures de prévention de la criminalité, du racisme et de la xénophobie, ainsi que de lutte contre ceux-ci, par des mesures de coordination et de coopération entre autorités policières et judiciaires et autres autorités compétentes, ainsi que par la reconnaissance mutuelle des décisions judiciaires en matière pénale et, si nécessaire, par le rapprochement des législations pénales. […] L'Union facilite l'accès à la justice, notamment par le principe de reconnaissance mutuelle des décisions judiciaires et extrajudiciaires en matière civile ».

15 Commission européenne, *Déclaration européenne sur les droits et principes pour la décennie numérique*, Bruxelles, 26 janvier 2022, COM (2022) 28 final.

16 D'autres exemples pourraient en effet être cités tels que le règlement DSA permettant de combattre notamment le cyberharcèlement : Parlement européen et Conseil, Règlement (UE) 2022/2065 du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE, JOUE L. 227/1, 25/10/2022.

17 F. Chaltiel, « Bilan et perspectives de la coopération européenne en matière de sécurité », *Actujuridique.fr*.

18 Parlement européen et Conseil de l'Union européenne, Règlement (UE) 2016/794 du 11 mai 2016 relatif à l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) et remplaçant et abrogeant les décisions du Conseil 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI et 2009/968/JA , *Journal officiel de l'Union européenne*, L 135, 24 mai 2016, p. 53-114, article 4.

19 480 voix pour, 143 contre et 20 abstentions.

20 Article 4, paragraphe 2 du Traité sur l'Union européenne et article 72 du Traité sur le fonctionnement de l'Union européenne.

21 Parlement européen et Conseil de l'Union européenne, Règlement (UE) 2018/1860 du 8 novembre 2018 relatif à l'utilisation du système d'information Schengen aux fins du retour des ressortissants de pays tiers en séjour irrégulier », *Journal officiel de l'Union européenne*, L 312/1, 17 décembre 2018, Parlement européen et Conseil de l'Union européenne, Règlement (UE) 2018/1861 du 28 novembre 2018, sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine des vérifications aux frontières, modifiant la convention d'application de l'accord Schengen et modifiant et abrogeant le règlement

(CE) nº 1987/2006 , *Journal officiel de l'Union européenne*, L 312/14, 7 décembre 2018, et Parlement européen et Conseil de l'Union européenne, Règlement (UE) 2018/1862 du 28 novembre 2018, sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine de la coopération policière et les coopérations judiciaires en matière pénale, modifiant et abrogeant le règlement CE nº 1986/2006 du Parlement européen et du Conseil et la décision 2010/261 :UE de la Commission , *Journal officiel de l'Union européenne*, L 312/56, 7 décembre 2018.

22 Art. R. 231-1 Code de la sécurité intérieure : « Le système d'information Schengen de deuxième génération (SIS II) a pour objet d'assurer un niveau élevé de sécurité dans l'espace de liberté, de sécurité et de justice de l'Union européenne, notamment la préservation de la sécurité et de l'ordre publics sur les territoires des États membres de l'espace Schengen ».

23 E. Aubin, « L'européanisation de la politique des visas : les nouvelles frontières du droit des étrangers », *RFDA*, 2017, nº 5, p. 917.

24 Voir notamment S. Merabet, *Vers un droit de l'intelligence artificielle*, Paris, Dalloz, coll. « Nouvelles bibliothèque des thèses », vol. 197, 2020.

25 Le caractère prédictif est en effet discuté.

26 Voir notamment en ce sens Assemblée nationale (Commission des lois), *Rapport d'information sur les enjeux d l'utilisation des images de sécurité dans le domaine public dans une finalité de lutte contre l'insécurité*, 12 avril 2023.

27 Les informations relatives au règlement sur l'IA sont à jour au 14 mai 2024.

28 Article 114-1 du TFUE : « Sauf si les traités en disposent autrement, les dispositions suivantes s'appliquent pour la réalisation des objectifs énoncés à l'article 26. Le Parlement européen et le Conseil, statuant conformément à la procédure législative ordinaire et après consultation du Comité économique et social, arrêtent les mesures relatives au rapprochement des dispositions législatives, réglementaires et administratives des États membres qui ont pour objet l'établissement et le fonctionnement du marché intérieur ».

29 Point 69 de la proposition de règlement

30 « un système d'identification biométrique à distance dans lequel l'acquisition des données biométriques, la comparaison et l'identification se

déroulent sans décalage temporel significatif. Cela comprend non seulement l'identification instantanée, mais aussi avec un léger décalage afin d'éviter tout contournement des règles » art. 9 pt. 37 de la proposition de règlement sur l'IA.

31 Commission européenne, *Proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle et modifiant certains actes législatifs de l'Union*, SEC (2021) final, Buxelles, 21 avril 2021, COM (2021), 206 final, article 47.

32 Résolution du Parlement européen, « L'intelligence artificielle en droit pénal et son utilisation par les autorités policières et judiciaires en matière pénale », *Parlement européen*, 2020/2016 (INI) – 06 octobre 2021

33 Voir notamment en ce sens Ph. Mouron et C. Piccio (dir.), *L'ordre public numérique*, PUAM, 2015.

34 L'Organisation des Nations unies la définit comme « tout comportement illégal faisant intervenir les opérateurs électroniques qui visent la sécurité des systèmes informatiques et des données qu'ils traitent », tandis que le ministère français de l'Intérieur la définit plus simplement comme l'ensemble des infractions pénales qui se commettent sur le réseau internet (www.interieur.gouv.fr), souligné par L. Burgorgue-Larsen, « Les nouvelles technologies », *Revue Pouvoirs*, 2009, nº 130, p. 65-80.

35 Parlement européen et Conseil européen, « Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 relative à des mesures pour un niveau commun élevé de cybersécurité dans l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 », JO L 333, 272022, p. 80.

36 Parlement européen et Conseil, « Directive (UE) 2016/1148 du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union », JO L 194, 19 juillet 2016, p. 1-30

37 Commission européenne, *Rapport de la Commission au Parlement européen et au Conseil évaluant la cohérence de l'approche adoptée par les États membres pour identifier les opérateurs de services essentiels conformément à l'article 23, paragraphe 1 de la directive 2016/1148/UE concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union*, Bruxelles, 28 octobre 2019, COM (2019) 546 final.

38 Parlement européen et Conseil européen, « Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 relative à des mesures pour un niveau commun élevé de cybersécurité dans l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 », *JO L 333*, 272022, p. 80.

39 L. BURGOGUE-LARSEN, « Les nouvelles technologies », *Revue Pouvoirs*, 2009, nº 130, p. 79.

40 Voir notamment en ce sens dans le champ spécifique de la sécurité : Parlement européen et Conseil, « Directive (UE) 2016/680 du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données », *Journal Officiel de l'Union européenne*, 2016, L. 119, p. 89.

41 Rapport de la Commission européenne au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, Commission européenne, « Protéger les droits fondamentaux à l'ère numérique », *Rapport annuel sur l'application de la Charte*, 2021, COM (2021) 819 final.

42 Le Parlement européen a adopté plusieurs résolutions sur la surveillance électronique de masse des citoyens.

43 J. SIRINELLI, « La protection des données de connexion par la Cour de justice : cartographie d'une jurisprudence européenne inédite », *RTD. Eur.*, avril-juin 2021, p. 313-329.

44 Parlement européen et Conseil européen « Directive 2009/136/CE, modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) nº 2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs », *Journal officiel de l'Union européenne*, 25 novembre 2009, L. 337/11, article 15 §1.

45 CJUE 8 avril 2014, aff. jointes C-293/12, C-594/12, Digital Rights Ireland et CJUE, 21 décembre 2016, Tele2 Sverige Tele2 Sverige AB, aff. C-203/15 et

Secretary of State for the Home Department, aff. C-698/15.

46 CJUE, 6 octobre 2020, Privacy International, aff. C-623/17, La Quadrature du Net, French Data Network, aff. C-511/18 et C-512/18. CJUE, 2 mars 2021, aff. C-746/18, Prokuratuur, Dalloz actu, 5 mars 2021, obs. B. Bertrand.

47 CJUE (Gde Ch.), 5 avril 2022, aff. C-140/20, GDC, *Dalloz*, obs. B. Bertrand.

48 *Charte des droits fondamentaux dans l'Union européenne*, 2021. Je souligne.

49 CE, ass, 21 avril 2021, n° 393099, French Data Network, J. Sirinelli et B. Bertrand, « Le Conseil d'État et la conservation des données de connexion : la quadrature du cercle », *Dalloz IP/IT*, 2021, p. 408.

50 *Loc. cit.*

51 Parlement européen et Conseil, « Directive (UE) 2016/680 du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil », L 119/89, 4 mai 2016.

52 CJUE, 30 janvier 2024, NG c/Direktor na Glavna direktsia « Natsionalna politsia » pri Ministerstvo na vatreshnite raboti – Sofia, aff. C-118/22.

53 Le Parlement a adopté plusieurs résolutions sur ces questions sensibles, notamment sur la surveillance électronique de masse des citoyens de l'Union européenne. L'objectif est de veiller à ce que les politiques en matière de sécurité soient conçues en tenant compte des droits fondamentaux.

54 D. Dero-Bugny, « Agences européennes », *JurisClasseur Europe*, Fasc. 245, 2016.

55 Conseil de l'Union européenne, Règlement (CE) n° 168/2007, 15 février 2007, *Journal officiel de l'Union européenne*, n° L 53, 22 février 2007, p. 1

56 Conseil de l'Union européenne, Règlement (CE) n° 2725/2000 du 11 décembre 2000 concernant la création du système « Eurodac » pour la comparaison des empreintes digitales aux fins de l'application efficace de la convention de Dublin, *Journal officiel des Communautés européennes*, n° L 316, 5 décembre 2000 p. 1-10

57 Parlement et Conseil européens, Règlement (UE) 2018/1725 du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) nº 45/2001 et la décision nº 1247/2002/CE », *Journal officiel de l'Union européenne*, L 295/39, 21 novembre 2018.

58 X. Dupré de Boulois., « Existe-t-il un droit à la sécurité publique ? », *RDLF*, 2018, chron nº 13.

ABSTRACTS

Français
Le caractère transnational des menaces qui pèsent sur la sécurité publique ou encore l'évolution de la nature de certaines menaces et infractions, ainsi que l'usage des nouvelles technologies pour les contrer contribuent à positionner l'Union européenne en la matière. L'Union européenne a pris des mesures importantes pour promouvoir l'utilisation des technologies numériques dans le domaine de la sécurité publique. Elle devient ainsi actrice de la sécurité publique aux côtés des États membres, mais elle tend également à s'affirmer comme protectrice des droits fondamentaux parfois en opposition aux États membres.

English
The transnational nature of the threats to public security and the changing nature of certain threats and offenses, as well as the use of new technologies to counter them, are helping to position the European Union on the matter. The European Union has taken important steps to promote the use of digital technologies in the field of public security.The European Union is thus becoming a player in public security alongside the member states, but it is also a fervent defender of fundamental rights, sometimes against the member states.

INDEX

Mots-clés
nouvelles technologies, surveillance biométrique, données personnelles, intelligence artificielle, droits fondamentaux

Keywords
new technologies, biometric surveillance, personal data, artificial intelligence, fundamental rights

AUTHOR

Mouna Mouncif-Moungache
Maître de conférences en droit public à l'Université Jean-Monnet Saint-Étienne
IDREF : https://www.idref.fr/113942605
ISNI : http://www.isni.org/0000000401522337
BNF : https://data.bnf.fr/fr/16665844