EDPS

CONTRÔLEUR EUROPÉEN
DE LA PROTECTION DES DONNÉES

RAPPORT ANNUEL 2022

RÉSUMÉ

Des informations supplémentaires sur le CEPD figurent sur notre site web à l'adresse: edps. europa.eu.

Le site web vous permet également de vous abonner à notre newsletter.

Waterford, Ireland – Bruxelles, Belgique: Trilateral Research Ltd, Vrije Universiteit Brussel, 2023

PRINT ISBN 978-92-9242-754-2 ISSN 1831-0516 doi: 10.2804/322163 QT-AB-23-001-FR-C

PDF ISBN 978-92-9242-736-8 ISSN 1977-8341 doi: 10.2804/509997 QT-AB-23-001-FR-N

AVANT-PROPOS

J'ai l'honneur de partager avec vous le rapport annuel 2022 du CEPD. Je repense à l'année écoulée avec beaucoup d'émotion, une année riche en événements, difficiles certes, mais prometteurs et encourageants, tant pour le monde dans son ensemble que pour le CEPD.

L'invasion de l'Ukraine par la Russie a suscité une réaction sans précédent de l'Union européenne (UE). Ce que l'UE a prouvé au cours de l'année écoulée, c'est qu'elle est capable de trouver des solutions à l'échelle de l'UE, en particulier face à des menaces extérieures, d'une manière qui non seulement prouve la solidarité, mais défend également nos valeurs et nos principes fondamentaux. C'est dans cet esprit que nous, au CEPD, avons également cherché à démontrer, tout au long de l'année écoulée, notre engagement pour le respect du droit fondamental à la protection des données, et ce même en temps de crise durant laquelle nos mesures et réponses ont dû être rapides et efficaces. Nos efforts pour soutenir les législateurs de l'UE dans le processus législatif et superviser le développement d'Eurojust, l'Agence de l'UE pour la coopération judiciaire en matière pénale, témoignent de notre conviction que nous sommes plus forts ensembles.

Malgré des événements mondiaux tumultueux, 2022 a également été une année d'aspirations et d'évolutions, un moment de réflexion sur la création d'un avenir apte à relever les défis d'aujourd'hui. Prenant la pleine mesure de la réalité de l'après-pandémie, nous avons organisé, les 16 et 17 juin à Bruxelles, une conférence intitulée «L'avenir de la protection des données: application effective dans le monde numérique», qui a réuni plus de 2 000 participants, en présentiel ou à distance, autour d'un objectif clé: faire avancer le débat sur l'avenir de l'application du règlement général sur la protection des données, quatre ans après son entrée en vigueur. Je suis fier de cet événement et des riches échanges qu'il aura permis pendant deux jours, et qui se sont soldés par des actions concrètes au sein de la communauté de la protection des données. Les engagements pris par le Comité européen de la protection des données dans sa déclaration du sommet de Vienne, ou l'intention de la Commission européenne de proposer une législation harmonisant certains aspects procéduraux de la coopération transfrontalière entre les autorités chargées de la protection des données, sont deux exemples importants des effets de cette conférence. Je suis curieux de voir où cette conversation nous mènera, et je suis reconnaissant à notre communauté dans son ensemble pour le courage dont elle a fait preuve dans ces réflexions.

En tant qu'autorité chargée de la protection des données qui supervise les institutions, organes et agences de l'UE, le CEPD a pour fonction particulière de contrôler de manière exclusive les autorités publiques: à ce titre, il lui incombe de contribuer à la réflexion sur le rôle de l'État dans une société démocratique. C'est ce qui nous a conduit, par exemple, à faire part de nos remarques préliminaires sur les logiciels espions modernes, avec pour objectif de contribuer à créer un meilleur contrôle démocratique des pratiques liées à l'application de la loi ou à la sécurité nationale.

Dans ce contexte, nous avons également ordonné à Europol de supprimer de grands ensembles de données dont les liens avec des activités criminelles n'avaient pas été établis. La réponse législative à cette question et la demande présentée par la suite par le CEPD devant la Cour de justice de l'Union européenne en vue de faire annuler les dispositions rétroactives du règlement Europol modifié témoignent de notre profonde conviction que l'Union européenne peut - et devrait - définir des normes mondiales en matière d'état de droit et de valeurs démocratiques.

Dans cet esprit, les normes les plus élevées doivent continuer à être recherchées au sein même de l'UE. Dans les années qui viennent, nous continuerons à faire tout ce qui est en notre pouvoir pour y parvenir. Je suis sûr que l'année prochaine apportera son lot de défis et de révélations, et je me réjouis à la perspective d'y faire face, avec l'ensemble de l'équipe dynamique et dévouée du CEPD.

Wojciech Wiewiórowski
Contrôleur européen de la protection des données

CHAPITRE I

À propos

1.1.
Le CEPD

Qui sommes-nous?

Le Contrôleur européen de la protection des données (CEPD) est l'autorité indépendante de l'Union européenne de la protection des données chargée de contrôler le traitement de données à caractère personnel par les institutions, organes et agences de l'Union européenne (les «institutions de l'UE»).

Nous offrons notre conseil aux institutions de l'UE sur les nouvelles propositions et initiatives législatives relatives à la protection des données à caractère personnel.

Nous suivons l'incidence des nouvelles technologies sur la protection des données et coopérons avec les autorités de contrôle afin de garantir l'application cohérente des règles de l'UE en matière de protection des données.

Notre mission

La protection des données est un droit fondamental protégé par la législation européenne. Nous veillons à développer une culture forte de la protection des données au sein des institutions de l'UE.

Nos valeurs et principes

Nous fondons notre travail sur quatre valeurs, à savoir:

- **Impartialité**: travailler au sein du cadre législatif et politique existant en faisant preuve d'indépendance et d'objectivité, trouver le juste équilibre entre les différents intérêts en jeu.
- **Intégrité**: respecter les normes de comportement les plus élevées et toujours faire ce qui est juste.
- **Transparence**: expliquer ce que nous faisons et pourquoi nous le faisons dans un langage clair et accessible à tous.
- **Pragmatisme**: comprendre les besoins des parties prenantes et rechercher des solutions qui fonctionnent dans la pratique.

Que faisons-nous?

Nos activités concernent quatre domaines principaux:

- **Contrôle et mise en application des règles**: nous contrôlons le traitement des données à caractère personnel par les institutions de l'UE et veillons à ce qu'elles respectent les règles en matière de protection des données.
- **Politique et consultation**: nous prodiguons des conseils à la Commission européenne, au Parlement européen et au Conseil sur des propositions et initiatives législatives liées à la protection des données.
- **Technologie et vie privée**: nous suivons et évaluons les évolutions technologiques qui ont une incidence sur la protection des données à caractère personnel. Nous veillons à ce que les systèmes qui sous-tendent le traitement des données à caractère personnel par les institutions de l'UE intègrent des fonctionnalités adéquates permettant de garantir le respect des règles en matière de protection des données. Nous mettons en œuvre la transformation numérique du CEPD.
- **Coopération**: nous travaillons avec les autorités chargées de la protection des données pour promouvoir une protection cohérente des données dans l'ensemble de l'UE. Notre principale plateforme de coopération avec les autorités chargées de la protection des données est le Comité européen de la protection des données, dont nous assurons le secrétariat, et avec lequel nous collaborons selon un protocole d'accord précis.

Nos pouvoirs

Les pouvoirs dont nous disposons en tant qu'autorité de protection des données des institutions de l'UE sont définis dans le règlement (UE) 2018/1725.

En application de ce règlement, nous pouvons, par exemple, prévenir ou adresser un avertissement à une institution de l'UE qui traite des données à caractère personnel de manière illicite ou déloyale; ordonner aux institutions de l'UE de se conformer à des demandes d'exercice de droits individuels; imposer une interdiction temporaire ou définitive à une opération de traitement de données particulière; infliger des amendes administratives aux institutions de l'UE; saisir la Cour de justice de l'Union européenne.

Nous disposons également de pouvoirs spécifiques pour contrôler la manière dont les organes et agences suivants traitent les données à caractère personnel: Europol – l'Agence de l'Union européenne pour la coopération des services répressifs au titre du règlement (UE) 2016/794; Eurojust – l'Agence de l'Union européenne pour la coopération judiciaire en matière pénale au titre du règlement (UE) 2018/1727; le Parquet européen, au titre du règlement (UE) 2017/1939; ainsi que Frontex – le corps européen de garde-frontières et de garde-côtes.

Pour plus d'informations sur le CEPD, nous vous invitons à consulter notre page Foire aux questions sur le site Internet du CEPD.

Pour en savoir plus sur la protection des données en général, nous vous invitons à consulter notre glossaire sur le site Internet du CEPD.

1.2.
Stratégie du CEPD pour la période 2020-2024

Dans un monde connecté, où les données traversent les frontières, la solidarité en Europe et au niveau international contribuera à renforcer le droit à la protection des données et à faire en sorte que les données bénéficient aux personnes de l'ensemble de l'UE et au-delà.

La stratégie du CEPD pour la période 2020-2024 repose sur trois piliers: **prospective**, **action** et **solidarité**, pour façonner un avenir numérique plus sûr, plus juste et plus durable.

- **Prospective**: notre engagement à être une institution qui agit avec discernement et adopte une vision à long terme des tendances de la protection des données et du contexte juridique, sociétal et technologique.

- **Action**: développer de manière proactive des outils pour que les institutions, organes et agences de l'UE soient les leaders mondiaux de la protection des données. Promouvoir la cohérence des activités des organes chargés de l'application de la législation dans l'UE avec l'expression renforcée d'une véritable solidarité européenne, d'un partage des tâches et d'une approche commune.

- **Solidarité**: nous pensons que la justice exige que la vie privée de tous soit préservée, dans toutes les politiques de l'UE, tandis que la viabilité devrait être le moteur du traitement des données dans l'intérêt public.

CHAPITRE II

Perspectives d'avenir: nos objectifs pour 2023 et au-delà

Examen à mi-parcours de notre stratégie – «Façonner un avenir numérique plus sûr»

La stratégie pour la période 2020-2024 «Façonner un avenir numérique plus sûr» a été élaborée à la veille d'une évolution mondiale. Rédigée début 2020, elle définissait trois piliers stratégiques pour le CEPD: **Prospective**, **Action** et **Solidarité**. Même nos meilleurs spécialistes de prospective n'auraient pu prévoir le changement de paradigme qui se préparait. La pandémie de COVID-19, la guerre en Ukraine et la crise économique mondiale ont tous constitué l'environnement difficile auquel nous avons été confrontés, au lendemain de l'adoption de notre stratégie 2020.

C'est pourquoi en 2022, nous avons décidé de procéder à un examen à mi-parcours de notre stratégie 2020-2024. Entrepris initialement dans le but d'évaluer les progrès accomplis dans la réalisation des objectifs définis dans cette stratégie, l'examen à mi-parcours a constitué un moment crucial pour déterminer si un changement d'orientation institutionnelle était nécessaire à la lumière de l'évolution de l'environnement mondial. Le chapitre suivant du présent rapport annuel reprend les résultats de cet examen à mi-parcours et expose la vision et les priorités recentrées du CEPD pour la suite de la mise en œuvre de la stratégie.

Procédure de l'examen à mi-parcours

Une approche ascendante (*bottom-up*) de l'examen à mi-parcours a été mise en œuvre et l'évaluation de la stratégie a été menée de l'intérieur. Cette décision a été adoptée dans l'intention de tirer parti des nouvelles perspectives du personnel du CEPD, en tenant compte de la croissance institutionnelle qui a eu lieu depuis 2020. Cette approche nous a permis de mettre à profit les connaissances et l'expérience interdisciplinaires internes du personnel du CEPD, afin de recenser les principaux domaines prioritaires pour nos activités dans les années qui viennent.

L'examen à mi-parcours a été réalisé en deux étapes. La première étape a consisté en une analyse des lacunes. Celle-ci a été réalisée sur la base d'un exercice de cartographie auquel l'ensemble du personnel du CEPD a participé. Le coup d'envoi a été officiellement lancé par une discussion entre le CEPD et le personnel, au cours de laquelle le Contrôleur a communiqué la procédure prévue pour une réflexion ouverte par le personnel. À la suite de précieuses contributions reçues au niveau du personnel, l'exercice de cartographie a été lancé. Celui-ci présentait une vue d'ensemble des 57 objectifs énumérés dans la stratégie du CEPD 2020-2024, le personnel du CEPD étant invité à réfléchir à la question de savoir, pour chacun de ces objectifs, si et dans quelle mesure il avait été atteint. À la suite de cette évaluation préliminaire, une analyse des lacunes a été réalisée pour déterminer l'état d'avancement des objectifs.

L'exercice de cartographie a permis de mettre en lumière les progrès substantiels accomplis pour atteindre et réaliser les objectifs définis dans la stratégie: en effet, sur ces 57 objectifs, l'analyse a révélé que 15 objectifs avaient été atteints jusqu'alors, que 40 étaient en cours de réalisation et que seuls 2 objectifs en étaient à un stade précoce de leur mise en œuvre.

Les résultats positifs de l'analyse ont jeté les bases de la deuxième étape de l'examen à mi-parcours. Au cours de cette deuxième étape, de nature consultative, le personnel du CEPD a été invité à s'exprimer sur l'avenir du CEPD et à réfléchir à la manière dont les nouvelles réalités de notre environnement pourraient justifier de revoir les priorités pour le reste de la stratégie. Une attention particulière a été accordée à la définition des domaines prioritaires sur lesquels le CEPD souhaiterait axer davantage ses efforts pour la suite de la stratégie.

Résultats de l'examen à mi-parcours: façonner un avenir numérique plus sûr et s'en faire le champion

La phase de consultation a vu l'émergence de plusieurs priorités institutionnelles, que nous considérons comme essentielles et auxquelles nous nous engageons à consacrer davantage d'attention et de ressources pour la suite de la stratégie 2020-2024.

Priorité n° 1: Application effective de la protection des données dans un nouveau paysage réglementaire

Avec l'adoption de multiples initiatives législatives dans le domaine numérique, le CEPD, à l'instar de la communauté des autorités chargées de la protection des données, évolue dans un environnement réglementaire nettement plus complexe. Ce nouveau paysage réglementaire qui compte, d'une part, des actes législatifs tels que le règlement sur la gouvernance des données (DGA), le règlement sur les marchés numériques (DMA) et le règlement sur les services numériques (DSA) et, d'autre part, les propositions de législation sur l'intelligence artificielle et de règlement sur les données, a amené le législateur à envisager de nouvelles fonctions et autorités réglementaires.

Bien que ces actes nouveaux ou à venir ne prévoient pas, en principe, d'entraver ni de modifier le RGPD (ou le RPDUE), ils contiennent plusieurs dispositions faisant explicitement référence aux définitions, notions et obligations prévues par le RGPD. En outre, si le traitement des données à caractère personnel s'inscrit au cœur des activités régies par chaque acte, les autorités chargées de la protection des données ne sont pas désignées comme étant les principales autorités compétentes. L'application de la législation est confiée, intégralement ou dans une très large mesure, à des autorités dont les missions portent essentiellement sur des objectifs politiques autres que la protection des données ou la vie privée. En conséquence, il est nécessaire de garantir une approche cohérente des activités réglementaires dans l'ensemble de la sphère numérique. Nous nous efforcerons donc de conceptualiser le rôle du CEPD à l'égard de ces autorités et de déterminer les attentes de celles-ci à l'égard du CEPD.

En nous appuyant sur notre expérience éprouvée et largement reconnue en matière de cohérence dans l'écosystème numérique, nous orienterons et participerons activement aux travaux des instances de coordination prévues par la loi, telles que le groupe de haut niveau sur le DMA et d'autres instances de coordination prévues par la législation, à la fois en tant que CEPD et en tant que membre du Comité européen de la protection des données, selon le cas.

Nous nous attacherons également à travailler en coopération étroite avec les organismes concernés dans les cas où aucun organe de coordination spécifique n'est pas prévu par la loi, mais où l'application de la législation nécessite un dialogue étroit avec les autorités chargées d'appliquer des dispositions ayant des implications en matière de protection de la vie privée et des données.

Nous veillerons également à ce que les principes et les règles en matière de protection des données ne soient pas compromis par l'application et le respect de la nouvelle législation. Le CEPD continuera donc à exercer sa fonction consultative afin de suivre et de mettre en lumière les conséquences potentielles découlant de la mise en œuvre pratique des nouveaux cadres réglementaires. Des mesures coercitives seront également envisagées en cas de besoin.

C'est dans ce contexte que le CEPD est en outre confronté à son rôle potentiel d'autorité de contrôle des institutions, organes et agences de l'UE en matière d'intelligence artificielle. D'un point de vue tant organisationnel que méthodologique, des préparatifs intensifs sont prévus pour nous assurer d'être prêts à remplir notre nouvelle mission dès le départ.

Le projet d'euro numérique revêt également une grande importance stratégique pour nous et nécessite une coopération étroite entre experts disposant d'une expertise politique, juridique, technologique et en matière de contrôle. Si bon nombre d'aspects dépendront des choix en matière de conception, le projet d'euro numérique aura indéniablement des implications importantes sur le respect de la vie privée et la protection des données. D'autres propositions concernant le secteur financier nécessiteront également un examen attentif, comme la proposition législative pour un cadre financier ouvert, qui entend permettre le partage des données et l'accès des tiers pour toute une gamme de secteurs et de produits financiers. Nous examinerons donc avec la plus grande attention les éventuelles interactions avec le règlement sur la gouvernance des données et le règlement sur les données.

La conférence du CEPD de juin 2022 sur «*L'avenir de la protection des données: application effective dans le monde numérique*», a considérablement contribué à faire avancer le débat public sur l'application du règlement général sur la protection des données (RGPD). Les évolutions en la matière, en particulier la déclaration du sommet de Vienne du Comité européen de la protection des données et la proposition annoncée de règlement harmonisant certains aspects des règles de procédure nationales de la Commission montrent que les efforts en faveur de l'amélioration du fonctionnement du RGPD continueront de dominer le débat dans les années qui viennent. Le succès de la conférence du CEPD, qu'il s'agisse de l'intérêt qu'elle a suscité auprès du public ou de ses retombées, montre que le CEPD, en tant qu'organe européen indépendant, a un rôle important à jouer dans ce débat en ce qui concerne la défense des approches paneuropéennes garantissant le plein respect de la charte des droits fondamentaux de l'Union européenne.

Priorité n° 2 : L'interopérabilité, un défi qui nécessite une approche de contrôle révisée

L'interopérabilité grandissante place le CEPD face à des obligations importantes pour garantir une approche efficace de contrôle. Avec l'introduction du cadre d'interopérabilité de l'UE, qui répond à une nouvelle approche de la gestion des données pour les frontières et la sécurité, nous devons également repenser la méthodologie du CEPD pour le contrôle des systèmes d'information à grande échelle. Les modifications proposées par ce cadre consisteraient à relier plusieurs systèmes d'information à grande échelle aux bases de données d'Europol et d'Interpol, ce qui constituerait un écosystème de flux de données qui amplifie les risques que l'exploitation des systèmes sous-jacents fait peser sur les personnes concernées.

Nous avons recensé plusieurs défis. Ainsi, la complexité de l'architecture globale et la fragmentation des règles en matière de protection des données appelle un recalibrage du contrôle, qui se concentre sur les flux de données plutôt que sur le contrôle distinct du traitement des données dans différents systèmes. De même, l'introduction d'activités supplémentaires de traitement de données qui n'étaient pas initialement prévues dans l'instrument juridique régissant la mise en place de chacun des systèmes d'information à grande échelle sous-jacents nécessite un examen approfondi du principe de limitation de la finalité. En outre, certaines décisions peuvent avoir une incidence considérable sur la protection des données en ce qui concerne les procédures de comitologie et le transfert de compétences à l'Agence de l'Union européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice (eu-LISA). L'absence d'un canal unique permettant aux personnes concernées d'exercer simultanément leurs droits dans tous les systèmes peut conduire à une fragmentation de ces droits.

Le CEPD se concentrera donc sur les trois domaines prioritaires suivants, qui constitueront le fondement de notre contrôle du cadre d'interopérabilité jusqu'à la fin du mandat:

(1) Droits des personnes concernées – Afin de faire face au risque de fragmentation des droits des personnes concernées due à la diversité des bases de données interopérables dotées de différents responsables du traitement, nous étudierons le potentiel d'un contrôle coordonné (y compris une réflexion conjointe avec les APD sur la rationalisation des procédures relatives aux droits des personnes concernées). En outre, nous nous efforcerons d'adopter une approche proactive en matière de droits des personnes concernées, en particulier le droit à l'information.

(2) Stratégie d'audit – Élaboration d'une stratégie sur mesure pour les audits relatifs à la protection des données dans les systèmes d'information à grande échelle et les éléments d'interopérabilité, adaptée au nouvel écosystème, ce qui pourrait donner lieu à l'abandon des systèmes d'audit cloisonnés en faveur des flux de données. Cette stratégie comprendra une approche commune du contrôle de l'interopérabilité en tenant compte également des nouvelles obligations d'audit à l'égard des agences de l'UE (Europol, Frontex, Eurojust), afin de garantir la limitation des finalités et de vérifier que ces entités accèdent aux données et les traitent conformément à leurs mandats respectifs. Cette approche commune comportera une partie juridique et une partie technique. En outre, étant donné que les règlements relatifs aux systèmes d'information à grande échelle demandent explicitement au CEPD d'effectuer des «*audits conformément aux normes internationales d'audit*», il sera nécessaire de dégager une interprétation commune de cette exigence.

(3) Profilage algorithmique – Le travail sur le profilage algorithmique visera en particulier à définir précisément la position du CEPD concernant l'application de cet outil dans le cadre de l'interopérabilité (ETIAS et VIS) et, plus généralement, se concentrera sur les questions de discrimination, de fiabilité, de proportionnalité et de transparence. Le contrôle du profilage algorithmique est une question complexe qui n'en est qu'à ses débuts et nécessite une coopération avec d'autres agences et organes dans le domaine des droits humains et de la non-discrimination, éventuellement avec d'autres acteurs de la société civile et du monde universitaire. Cette surveillance soutiendra notre contribution aux travaux de l'ETIAS, le système européen d'information et d'autorisation concernant les voyages, et des comités d'orientation sur les droits fondamentaux du système d'information sur les visas, et visera à mettre au point des outils de suivi et de contrôle appropriés pour ce nouveau domaine.

Priorité n° 3: Une coopération internationale pour promouvoir des approches mondiales communes face aux défis en matière de protection de la vie privée et des données

Nous estimons qu'il est fondamental de s'impliquer activement dans une coopération internationale qui nous permettra d'interagir avec une communauté plus large, au-delà des frontières de l'Europe, et de promouvoir une compréhension et des approches communes face aux défis de la protection des données et de la vie privée. Nous prévoyons d'intensifier nos efforts dans le domaine de la coopération internationale étant donné que plusieurs questions de haute importance stratégique sont traitées dans les enceintes internationales.

En particulier, nous entendons favoriser la coordination des actions et de la stratégie des membres du Comité européen de la protection des données dans les enceintes internationales, de poursuivre les travaux menés dans le cadre de la GPA (Global Privacy Assembly), du Conseil de l'Europe, ainsi que de la table ronde des APD du G7, et de l'Organisation de coopération et de développement économiques (OCDE), en veillant à une participation active et à une véritable représentation des points de vue des autorités européennes et du Comité européen de la protection des données. Nous nous efforcerons également de renforcer la coopération avec les organisations internationales ainsi qu'avec les réseaux régionaux de protection des données.

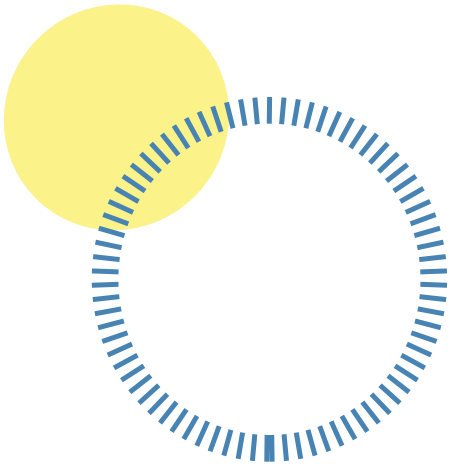
Priorité n° 4: Repenser les processus du CEPD afin de garantir l'efficacité dans un monde en mutation rapide

La mise en œuvre de la stratégie 2020-2024 du CEPD se déroule sur fond de crises successives. De la pandémie de COVID-19 à l'invasion de l'Ukraine par la Russie, en passant par la hausse des coûts de l'énergie et l'inflation, nous avons dû adapter nos méthodes et processus de travail afin de continuer à assurer nos missions. Si nous sommes parvenus, en principe, à respecter les engagements pris dans le cadre de notre stratégie, l'analyse interne montre qu'il est nécessaire de poursuivre le réajustement de certains processus, afin d'améliorer notre efficacité et nos normes à long terme, à la fois en tant qu'administration publique de l'UE et en tant qu'autorité chargée de la protection des données.

Dans ce dernier cas, cela concerne, entre autres, des éléments livrables tels que le suivi des notifications de violation de données, le règlement des plaintes ou la capacité de cibler de manière proactive des sujets critiques liés à la conformité au moyen d'enquêtes ou d'audits. Une réflexion plus approfondie sera menée sur de nouveaux outils permettant une évaluation en ligne ou à distance de la conformité. Parallèlement, les contraintes en matière de ressources humaines et budgétaires constituent un obstacle important à l'exécution des missions de contrôle du CEPD.

Dans le même ordre d'idées, avec la guerre en Ukraine, le CEPD se voit confier de nouvelles tâches autonomes. En 2021, la Commission européenne a proposé un train de mesures législatives visant à modifier le règlement Eurojust afin de permettre le traitement des preuves recueillies aux fins d'enquêter sur les crimes de guerre commis par la Russie. En 2022, une autre modification législative a été adoptée, désignant Eurojust comme pôle européen pour la conservation, le stockage et l'analyse des preuves relatives aux grands crimes internationaux. Le CEPD s'est vu attribuer un rôle important dans la mise en place de la nouvelle base de données probantes. En janvier 2023, la Commission européenne a annoncé la création du centre international pour les poursuites relatives aux crimes d'agression contre l'Ukraine (ICPA) au sein d'Eurojust. L'ensemble de ces évolutions législatives ont déjà donné lieu ou donneront lieu à des tâches supplémentaires considérables pour l'ensemble de nos équipes. Compte tenu de l'importance politique du soutien de l'UE à l'Ukraine, ainsi que de la charge de travail considérable qui y est associée, nous traiterons les activités dans ce domaine comme l'une de nos principales priorités.

Compte tenu de l'intérêt croissant du public pour les travaux du CEPD, comme le montre, entre autres, le nombre de demandes d'accès aux documents, nous nous engageons également à respecter des normes de transparence plus strictes, non seulement dans le cadre d'une bonne administration, mais aussi en tant que moyen important de rendre notre travail accessible aux personnes. Nous nous engageons également à continuer de garantir des niveaux élevés de protection des données et de responsabilité, et à montrer l'exemple non seulement en respectant les exigences légales, mais aussi en explorant et en utilisant des outils et des services d'excellence respectueux de la vie privée et de la protection des données. En ce qui concerne la cybersécurité, nous devrons nous adapter aux nouveaux règlements visant à garantir un niveau commun élevé de cybersécurité dans l'ensemble des institutions de l'UE.



CHAPITRE 3

Événements marquants en 2022

3.1.
Utiliser nos pouvoirs pour protéger les personnes

En tant qu'autorité de contrôle de la protection des données chargée de superviser les institutions, organes et agences de l'UE (les institutions de l'UE), notre objectif est de veiller à ce qu'ils respectent la législation de l'UE en matière de protection des données, afin de protéger les personnes et leurs droits fondamentaux au respect de la vie privée et à la protection des données.

Pour y parvenir, nous fournissons aux institutions de l'UE des orientations, formulons des recommandations, des commentaires et des avis, effectuons des audits, offrons des sessions de formation, ainsi que d'autres ressources, afin de les doter des outils appropriés pour mettre en pratique la protection des données dans le cadre de leurs tâches et décisions courantes nécessitant le traitement de données à caractère personnel.

3.1.1.
Contrôle de l'espace de liberté, de sécurité et de justice

Parmi les thèmes sur lesquels notre intervention s'est avérée nécessaire, nous avons accordé une attention particulière au contrôle de l'espace de liberté, de sécurité et de justice (ELSJ) de l'UE, qui couvre des domaines d'action allant de la gestion des frontières extérieures à la coopération judiciaire en matière civile et pénale, en passant par l'asile, la migration et la lutte contre la criminalité. L'ELSJ comprend des agences de l'UE, telles qu'Europol – l'Agence de l'UE pour la coopération des services répressifs, Frontex – l'Agence européenne de garde-frontières et de garde-côtes, le

Parquet européen, et Eurojust – l'Agence de l'UE pour la coopération judiciaire en matière pénale. Notre rôle dans ce domaine a donc été particulièrement important, compte tenu du caractère sensible des informations traitées et de l'incidence considérable que cela pourrait avoir en cas de mauvaise gestion.

3.1.2.
Transferts de données à caractère personnel vers des pays non membres de l'UE/EEE

La question des transferts internationaux de données à caractère personnel vers des pays situés en dehors de l'UE ou de l'Espace économique européen (EEE) a également été de plus en plus présente au fil des ans, y compris en 2022, ce qui nous a amenés à mobiliser des ressources considérables afin de garantir un niveau de protection des données à caractère personnel adéquat.

À cette fin, nous avons mené un certain nombre d'initiatives et fourni des conseils et des recommandations sur la manière dont les institutions de l'UE devraient satisfaire aux exigences de la législation de l'UE en matière de protection des données lorsqu'elles utilisent des services ou concluent des contrats avec des entités situées en dehors de l'UE/EEE.

L'utilisation de produits et services non-UE/EEE

Parmi nos initiatives figurent nos enquêtes en cours sur l'utilisation par les institutions de l'UE de produits et de services en nuage provenant d'entités établies en dehors de l'UE/EEE, en particulier l'utilisation de Microsoft Office 365 par la Commission européenne, la publication de lignes directrices et de politiques, ainsi que la fourniture de formations aux institutions de l'UE. Ces efforts visent à sensibiliser

les institutions de l'UE aux risques posés par l'utilisation d'outils ou la réalisation d'activités de traitement de données impliquant des transferts de données en dehors de l'UE/EEE. Nous entendons également sensibiliser les institutions de l'UE aux clauses contractuelles et aux ententes administratives, ainsi qu'à d'autres mesures visant à garantir que les données à caractère personnel des personnes soient protégées d'une manière essentiellement équivalente en dehors de l'UE/EEE.

Dans le cadre de nos travaux dans ce domaine, et à la lumière de nos compétences au sein du CEPD, nous avons autorisé un certain nombre de transferts de données à caractère personnel vers des pays tiers ou de l'EEE, où les institutions de l'UE ont été en mesure de prouver l'existence de procédures et de mesures solides permettant de garantir que ces transferts garantissent la protection des données à caractère personnel des personnes.

Dans le but de montrer l'exemple dans ce domaine, nous nous attelons également à l'utilisation de produits et de services de substitution basés dans l'UE/EEE, et nous encourageons les institutions de l'UE à tenir également compte de cet aspect.

3.1.3.
Audit des systèmes d'information à grande échelle

L'une de nos principales missions consiste à garantir la protection des données à caractère personnel et de la vie privée dans le contexte des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice. L'une de nos fonctions consiste à procéder à l'audit de ces systèmes afin de s'assurer qu'ils sont conformes aux réglementations en matière de protection des données et de respect de la vie privée.

Dans le cadre de cette fonction, nous évaluons les mesures techniques et organisationnelles mises en place par les opérateurs système, en veillant à ce que les systèmes soient conçus selon le principe du respect de la vie privée dès la conception. Nous encourageons également les bonnes pratiques en partageant les conclusions et les recommandations des audits avec d'autres autorités de l'UE chargées de la protection des données, favorisant ainsi une culture de l'excellence en matière de protection des données et de respect de la vie privée dans l'ensemble de l'UE.

Grâce à cette activité, nous nous efforçons de sensibiliser les institutions de l'UE et le grand public à l'importance de la protection des données et de la vie privée dans les systèmes d'information à grande échelle. Nous contribuons à protéger les informations à caractère personnel des citoyens de l'UE et veillons à ce que les systèmes d'information à grande échelle respectent les normes les plus élevées en matière de protection des données et de respect de la vie privée.

En octobre 2022, nous avons procédé à l'audit de trois systèmes d'information à grande échelle dans les locaux de l'agence eu-LISA – Agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice, à Strasbourg:

Eurodac, la base de données de dactyloscopie européenne en matière d'asile, utilisée pour le traitement des demandes d'asile.

Le **SIS II**, qui soutient la sécurité intérieure et l'échange d'informations sur les personnes et les objets entre la police nationale, le contrôle aux frontières, les douanes, les autorités chargées des visas et les autorités judiciaires.

Le **VIS**, qui soutient l'application de la politique commune de visas de l'UE et facilite les contrôles aux frontières et la coopération consulaire.

L'audit comprenait notamment un examen de la méthodologie et des pratiques employées par eu-LISA pour développer et tester les systèmes tout en veillant à ce que les principes de sécurité et de protection des données dès la conception et par défaut soient appliqués. En outre, nous avons contrôlé les mesures relatives à la gouvernance de la sécurité informatique, aux incidents de sécurité et aux violations de données à caractère personnel, et nous avons contrôlé l'application des recommandations issues de nos précédents audits.

3.2.
Protéger notre indépendance

Nouveau règlement Europol: recours du CEPD devant la Cour de justice de l'Union européenne

Le 16 septembre 2022, nous avons demandé à la Cour de justice de l'Union européenne (CJUE) d'annuler deux dispositions du règlement Europol nouvellement modifié, entré en vigueur le 28 juin 2022 (affaire T-578/22 – CEPD/Parlement et Conseil). Ces deux dispositions ont une incidence sur les opérations de traitement de données à caractère personnel effectuées par le passé par Europol. Elles portent gravement atteinte à la sécurité juridique des données à caractère personnel des personnes et menacent l'indépendance du CEPD.

3.3.
Façonner un avenir numérique plus sûr

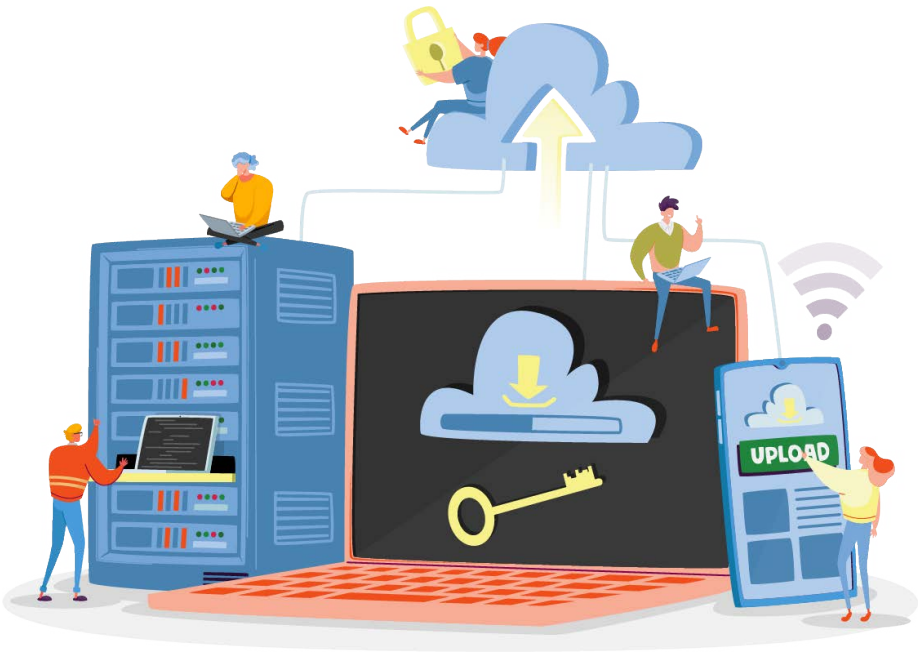
Comme indiqué dans notre stratégie 2020-2024, nous apprécions les initiatives dans lesquelles les données générées en Europe sont converties en valeur pour les entreprises et les particuliers européens, et traitées selon les valeurs européennes, afin de façonner un avenir numérique plus sûr. Suivant cette orientation, nous avons fourni des conseils au législateur de l'UE sur un large éventail de questions, notamment la santé, l'intelligence artificielle et les initiatives visant à lutter contre la criminalité.

En principe, nos conseils au législateur de l'UE sur les propositions législatives revêtent la forme d'avis ou d'observations formelles. Nos **avis** sont émis en réponse à des demandes obligatoires de la Commission européenne, qui est légalement tenue de solliciter nos orientations sur toute proposition législative, ainsi que des recommandations et propositions adressées au Conseil dans le cadre d'accords internationaux ayant une incidence sur la protection des données. **Les commentaires formels** sont émis en réponse à une demande de la Commission européenne sur des projets d'actes d'exécution ou d'actes délégués.

Lorsqu'une proposition législative ou autre proposition pertinente revêt une importance particulière pour la protection des données à caractère personnel, la Commission européenne peut également consulter le Comité européen de la protection des données. Dans de tels cas, le CEPD et le Comité européen de la protection des données travaillent ensemble à l'élaboration d'un **avis conjoint**.

Le règlement de l'UE sur les données

Nous avons publié un avis conjoint avec le Comité européen de la protection des données sur la proposition de règlement sur les données, qui vise à établir des règles harmonisées concernant l'accès aux données générées à partir d'un large éventail de produits et services, y compris les objets connectés («internet des objets»), les dispositifs médicaux ou de santé et les assistants virtuels, et leur utilisation.



L'avis souligne que les données doivent être traitées conformément aux valeurs européennes si nous avons pour ambition de façonner un avenir numérique plus sûr. Alors que de nouvelles possibilités d'utilisation des données apparaissent, il convient de veiller à ce que le cadre existant en matière de protection des données demeure totalement intact. Nous avons également souligné que l'accès aux données par les autorités publiques devrait toujours être correctement défini et limité à ce qui est strictement nécessaire et proportionné, ce qui n'est pas le cas si l'on en croit le projet de règlement sur les données.

L'espace européen des données de santé

Nous avons également publié un avis conjoint sur la proposition relative à l'espace européen des données de santé, dans lequel nous préconisons une protection renforcée des données de santé électroniques.

La proposition relative à l'espace européen des données de santé est la première d'une série de propositions concernant des espaces européens communs de données spécifiques à un domaine. Elle fera partie intégrante de la construction d'une Union européenne de la santé visant à permettre à l'UE d'exploiter pleinement le potentiel offert par un échange, une utilisation et une réutilisation sûrs et sécurisés des données relatives à la santé.

Conjointement avec le Comité européen de la protection des données, nous avons fait part de plusieurs préoccupations, notamment en ce qui concerne l'utilisation secondaire des données de santé électroniques.

Intelligence artificielle

Comme le souligne notre stratégie 2020-2024, l'intelligence artificielle est de plus en plus déployée dans les services publics et la justice pénale. Notre rôle est de veiller à ce que cette nouvelle technologie soit utilisée conformément à la législation de l'UE en matière de protection des données et respecte la vie privée des personnes.

Outre d'autres initiatives que nous avons lancées ou auxquelles nous avons participé, nous avons publié un avis sur la recommandation de décision du Conseil autorisant l'ouverture de négociations au nom de l'Union européenne en vue d'une convention du Conseil de l'Europe sur l'intelligence artificielle, les droits de l'homme, la démocratie et l'État de droit (convention sur l'IA), que nous considérons comme une étape

importante dans l'élaboration du premier instrument international juridiquement contraignant sur l'IA conformément aux normes et valeurs européennes en matière de droits de l'homme, de démocratie et d'État de droit, qui complète la législation de l'UE sur l'intelligence artificielle. Néanmoins, nous avons insisté sur la nécessité de prévoir des garanties appropriées, solides et claires en matière de protection des données afin de protéger les personnes susceptibles d'être affectées par l'utilisation de systèmes d'IA.

Lutte contre la criminalité

Nous avons publié une sélection d'avis sur diverses propositions dans le domaine du droit pénal.

Par exemple, l'un de nos avis, publié conjointement avec le Comité européen de la protection des données, portait sur une proposition de règlement visant à prévenir et à combattre les abus sexuels commis contre des enfants: nous avons exprimé notre soutien aux objectifs et aux buts de cette proposition, tout en faisant part de notre inquiétude quant au fait qu'elle puisse présenter davantage de risques pour les personnes et, par extension, pour la société dans son ensemble, que pour les criminels poursuivis pour abus sexuels sur enfants.

Un autre exemple notable de cas dans lequel nous avons formulé des recommandations et des orientations concernait le thème de la coopération internationale en matière de lutte contre la criminalité. En particulier, nous avons publié un avis sur deux propositions: l'une visant à autoriser les États membres de l'UE à signer le deuxième protocole additionnel à la convention de Budapest sur la cybercriminalité, et l'autre à autoriser les États membres de l'UE à ratifier ce même protocole.

Si les enquêtes et les poursuites pénales constituent un objectif légitime pour lequel la coopération internationale, y compris l'échange d'informations, joue un rôle important, nous avons souligné l'importance pour l'UE de conclure des accords durables pour le partage de données à caractère personnel avec des pays tiers à des fins répressives. Ces accords devraient être pleinement compatibles avec le droit de l'Union, y compris les droits fondamentaux au respect de la vie privée et à la protection des données.

3.4.
L'avenir de la protection des données: application effective dans le monde numérique

En juin 2022, nous avons organisé notre conférence du CEPD, intitulée «L'avenir de la protection des données: application effective dans le monde numérique», qui a rassemblé plus de 2 000 participants, à Bruxelles et en ligne, avec au programme: plus d'une centaine d'intervenants; trois sessions principales; seize sessions-débats; neuf allocutions individuelles; et cinq événements parallèles. Cet événement de deux jours a permis la tenue de discussions cruciales sur l'avenir de la protection des données, en mettant particulièrement l'accent sur l'application du règlement général sur la protection des données (RGPD).

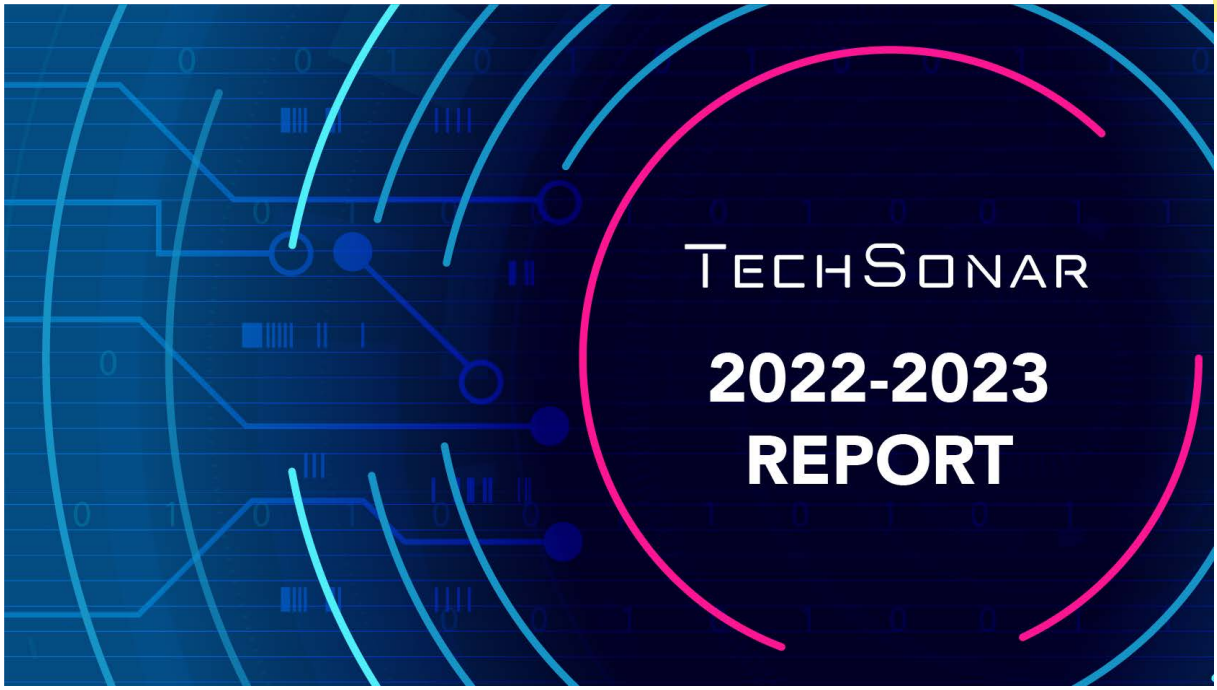
Notre vision à long terme de l'avenir de la protection des données est claire: il est nécessaire de traiter l'application de la législation de manière paneuropéenne afin de garantir un niveau élevé et réel de protection des personnes et d'honorer les promesses du RGPD.

3.5.
Veille et prospective technologique

L'un des trois piliers fondamentaux de la stratégie du CEPD pour la période 2020-2024 est la **prospective**, à savoir notre détermination à être une institution intelligente qui adopte une vision à long terme des tendances en matière de protection des données et du contexte juridique, sociétal et technologique.

L'un des moyens que nous mettons en pratique en matière de prospective consiste à dialoguer avec des experts, des spécialistes et les autorités chargées de la protection des données. Notre objectif est de comprendre les technologies, d'analyser leurs répercussions en matière de respect de la vie privée et de protection des données pour les personnes, dans le but de partager les connaissances et de pousser le développement de ces technologies nouvelles et émergentes vers le respect de la vie privée. **TechSonar** et **TechDispatch** sont deux de nos initiatives dans ce domaine.

TechSonar vise à anticiper les tendances technologiques émergentes, afin de mieux comprendre les évolutions futures du secteur des technologies du point de vue de la protection des données. Sur la base de notre effort collectif, grâce à la découverte de tendances, à la réflexion, à l'examen, à la publication, à la sensibilisation et à un suivi continu, nous entendons contribuer au débat plus large sur la prospective au sein des institutions de l'UE. Publié le 10 novembre 2022, le deuxième rapport annuel TechSonar présente en détail cinq technologies qui méritent d'être suivies au cours de l'année à venir. Il s'agit de la monnaie numérique de banque centrale, du métavers, des données synthétiques, de l'apprentissage fédéré et des systèmes de détection des fausses informations.



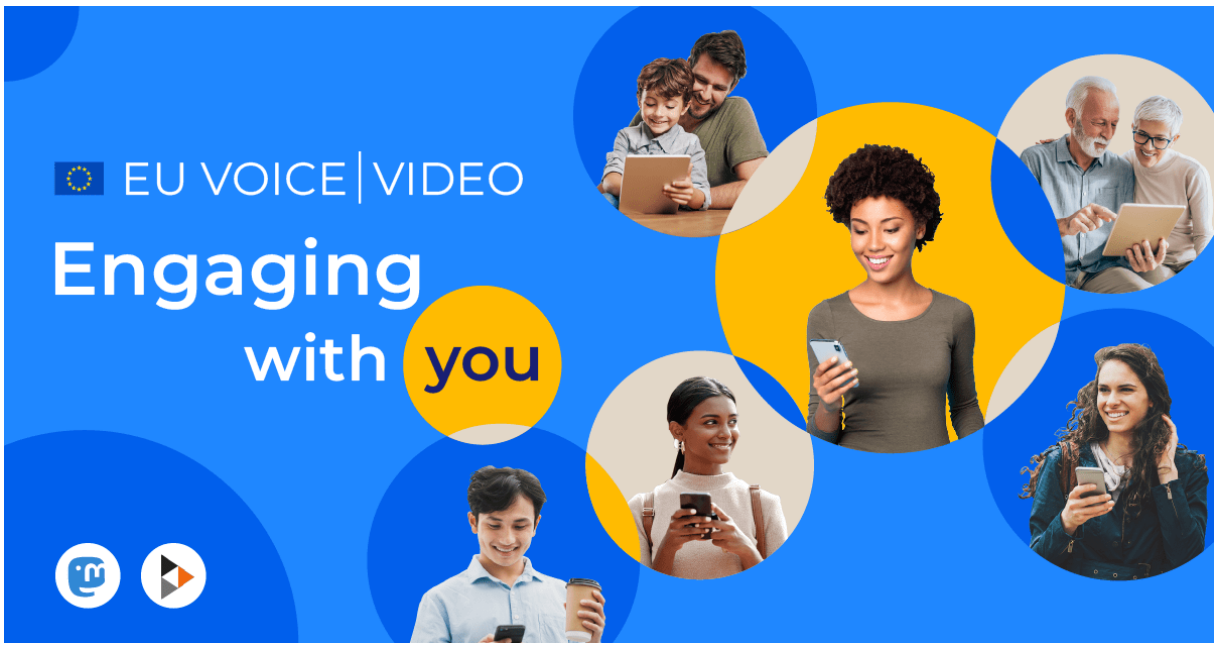
TechDispatch vise à expliquer les évolutions technologiques émergentes. Les rapports TechDispatch, pour lesquels nous avons remporté le prix de la Global Privacy Assembly en 2021, s'inscrivent dans le cadre plus large des activités du CEPD en matière de veille technologique. Chaque TechDispatch fournit des descriptions factuelles d'une nouvelle technologie, évalue à titre préliminaire les incidences possibles sur la vie privée et la protection des données à caractère personnel, telles que nous les comprenons actuellement, et fournit des liens vers des lectures recommandées. L'édition de cette année de TechDispatch, publiée en juillet 2022, porte essentiellement sur les réseaux sociaux fédérés (fediverse) et les plateformes de médias sociaux fédérées.

3.6.
Innovation numérique

Promouvoir des outils conviviaux en matière de protection des données qui respectent et privilégient les droits fondamentaux des personnes tout au long de leur développement et de leur utilisation est l'un des objectifs essentiels de notre stratégie pour la période 2020-2024. Pour atteindre ces objectifs, nous avons cherché et continuons à rechercher d'autres outils, notamment des outils de communication et de collaboration, conformes aux lois et aux normes de l'UE en matière de protection des données. En utilisant ces autres outils nous-mêmes, nous tentons d'encourager les institutions de l'UE à suivre notre exemple. Ainsi, nous pouvons collectivement minimiser notre dépendance à l'égard des prestataires en position de monopole, afin d'éviter un verrouillage préjudiciable.

Nous jouons un rôle important dans la promotion de l'innovation numérique en montrant l'exemple, notamment en utilisant des applications et des plateformes de source ouverte qui offrent des alternatives respectueuses de la vie privée aux produits et services fournis par de grandes entreprises technologiques. Notre engagement en faveur de la protection de la vie privée s'étend à la fois aux réseaux sociaux et aux outils de collaboration, avec des initiatives telles que EU Video, EU Voice et les projets pilotes Nextcloud.

En février 2022, nous avons lancé la phase pilote de deux plateformes de médias sociaux: EU Voice, pour publier des publications régulières sur nos activités, et EU Video, pour publier des vidéos, en tant que canaux de communication supplémentaires et alternatifs pour interagir avec notre public. Ces deux plateformes font partie de réseaux sociaux décentralisés, gratuits et de source publique, qui connectent les utilisateurs dans un environnement privilégiant la protection de la vie privée, basé sur les logiciels Mastodon et PeerTube. Les deux projets mettent l'accent sur la protection des données et la vie privée des utilisateurs, en veillant à ce que les institutions de l'UE aient accès à des outils de communication conformes aux valeurs et aux principes européens, sans compromettre leurs informations à caractère personnel.



Outre les réseaux sociaux, nous encourageons l'adoption d'outils de collaboration alternatifs qui accordent à la protection de la vie privée une place de premier plan. Le projet pilote Nextcloud illustre parfaitement cet engagement. Nextcloud est une plateforme en nuage auto-hébergée, de source publique, qui permet aux utilisateurs de stocker, et partager en toute sécurité des fichiers, des calendriers et des contacts, et de collaborer de manière sûre sur ces derniers. En promouvant et en utilisant des outils respectueux de la vie privée tels que Nextcloud, nous faisons preuve d'un engagement en faveur d'un écosystème numérique qui préserve les principes de protection des données et de la vie privée, favorisant à terme le développement d'alternatives innovantes et plus respectueuses de la vie privée.

En juin 2022, au cours de la conférence du CEPD intitulée «L'avenir de la protection des données: application effective dans le monde numérique», nous avons également mis au point une solution de vidéoconférence sur mesure qui respectait pleinement les exigences en matière de transfert de données prévues par le RGPD et le règlement r(UE) 2018/1725, ce qui nous a permis de montrer l'exemple et d'ouvrir la voie au respect des exigences en matière de protection des données. En tant qu'autorité de protection des données chargée de contrôler toutes les institutions de l'UE, nous tenions à montrer qu'il est possible de faire preuve d'une conformité exemplaire en ce qui concerne les outils de vidéoconférence et, en particulier, de respecter les règles en matière de transferts de données lors des transferts de données à caractère personnel vers des pays hors UE et EEE.

3.7.
Communiquer sur la protection des données

L'un de nos objectifs, en tant qu'organisation, est d'expliquer ce que nous faisons et pour quelles raisons, de manière transparente, claire et interactive, car il est important pour les citoyens de l'UE de comprendre leurs droits en matière de protection des données et la manière dont ils peuvent être affectés.

Une présence de plus en plus croissante en ligne

Le CEPD jouit d'une solide présence sur plusieurs réseaux sociaux, à savoir Twitter (29,1k), LinkedIn où nous avons dépassé les 63 000 abonnés cette année, YouTube (2,75k), EU Voice (5,1k) et EU Video (0,69k) grâce auxquels nous sommes en mesure d'atteindre un public international facilement et rapidement.

De manière générale, nous créons du contenu pour promouvoir des campagnes de visibilité et rendre compte en direct de la participation du CEPD à divers événements.

La protection des données au plus près du public

La protection des données peut parfois s'avérer assez complexe; par conséquent, nous nous efforçons d'émettre des contenus qui conviennent tant aux experts qu'aux non-spécialistes en matière de protection des données, en rapprochant nos activités du public.

Cette approche implique notamment la production de bulletins d'information mensuels, la fourniture d'explications succinctes sur nos dernières initiatives et sur la manière dont elles peuvent avoir une incidence sur le public, la production de fiches d'information dans lesquelles nous décomposons des concepts clés en matière de protection des données, ainsi que l'organisation de campagnes sur les médias sociaux, et la collaboration avec d'autres institutions de l'UE pour sensibiliser aux questions relatives à la protection des données. Dans le même esprit, nous avons lancé cette année une nouvelle série de podcasts, la Newsletter Digest, afin de toucher un public plus large, en l'informant de ce que nous faisons pour la protection des données.

Médias et relations publiques

Nous échangeons fréquemment avec les médias, plus particulièrement par l'intermédiaire de communiqués de presse sur les initiatives importantes en matière de protection des données qui ont un vaste impact à l'échelle de l'UE. Cette année, plusieurs questions ont fait l'objet d'une attention particulière, accompagnée de mesures de suivi ou de demandes d'entretiens, telles que la supervision d'Europol et de Frontex, ou notre conférence du mois de juin.

De même, nous entretenons notre relation avec le public, en répondant à ses demandes sur notre travail et nos compétences en tant qu'institution de l'UE et en organisant des visites dans nos locaux.

Reprendre le rythme après la COVID-19

Du fait de la réduction progressive des restrictions liées à la COVID-19, nous avons pu recommencer à organiser des événements, accroître le nombre d'activités en présentiel tout en continuant à les adapter à un monde post-COVID. Nos manifestations et activités ont été conçues de manière à ce que l'on puisse y participer en ligne ou en présentiel, ce qui nous a aidés à réduire notre impact environnemental en tant qu'organisation. Il convient de noter que nous avons accueilli avec succès deux grands événements hybrides: la conférence sur «L'avenir de la protection des données. application effective dans le monde numérique», en juin 2022, qui a réuni 2 000 personnes en ligne et en présentiel, et notre «conférence concernant le contrôle: protection des données et justice

pénale» en novembre 2022, à laquelle ont participé plus de 200 personnes, à distance et en présentiel. Dans la plupart des cas, nous avons fait de notre mieux pour rendre ces événements plus «écologiques» en faisant appel à des services de restauration locaux, en évitant le gaspillage alimentaire et en nous procurant nos documents promotionnels auprès de prestataires locaux, fabriqués à partir de matériaux réutilisables.

Communication collaborative

En 2022, nous avons travaillé avec d'autres institutions de l'UE sur des activités de communication communes. En octobre, nous avons uni nos forces à celles de l'ENISA, l'Agence de l'Union européenne pour la cybersécurité, et de la Commission européenne, pour proposer une campagne pour le mois européen de la cybersécurité (ECSM), marquant ainsi son 10e anniversaire. Par ailleurs, nous avons apporté des idées et un soutien en matière de protection des données à la commission inter-institutionnelle de communication en ligne (IOCC). Dans le cadre du projet pilote EU Voice et EU Video notamment, nous avons coopéré étroitement avec l'IOCC afin de formuler des orientations éditoriales et des politiques concernant les serveurs et d'aider les institutions de l'UE à s'impliquer dans le projet.

3.8.
Une organisation en évolution

Pour soutenir nos objectifs, en particulier ceux énoncés dans notre stratégie pour la période 2020-2024, nous avons élargi et fait évoluer notre organisation de sorte qu'elle reflète davantage notre manière de travailler.

Nous avons adapté l'organisation interne du CEPD, en créant un service juridique à part entière, ainsi que le secteur «Gouvernance et conformité interne», afin de disposer de l'expertise nécessaire pour mener à bien certaines tâches.

Atteindre nos objectifs signifie également que nous devons gérer nos ressources avec prudence. À cet égard, des efforts considérables ont été consacrés à la planification, à l'exécution et à l'audit de notre budget.

Nous avons également entrepris les préparatifs nécessaires à l'ouverture d'un bureau de liaison du CEPD à Strasbourg, qui sera officiellement inauguré début 2023, afin de renforcer la coopération interinstitutionnelle et la coopération internationale et de pouvoir fournir un soutien consultatif supplémentaire sur les questions de protection des données.

Indicateurs clés de performance 2022

Nous utilisons un certain nombre d'indicateurs clés de performance (ICP) afin de mieux cerner les résultats de notre action au regard des principaux objectifs définis dans la stratégie du CEPD. Nous garantissons ainsi notre capacité à adapter nos activités, si nécessaire, pour accroître l'impact de nos travaux et l'efficacité de notre utilisation des ressources.

Le tableau de bord des ICP, reproduit ci-après, comprend une description succincte de chaque ICP et les résultats obtenus au 31 décembre 2022. Ces résultats sont mesurés par rapport aux objectifs initiaux, ou par rapport aux résultats de l'année précédente, utilisés comme indicateur.

En 2022, nous avons atteint ou dépassé (dans certains cas de manière significative) les objectifs fixés dans huit des neuf ICP, sauf un ICP (l'ICP 8) concernant le taux d'occupation du tableau des effectifs. Ces résultats illustrent bien la voie positive que nous avons suivie dans la mise en œuvre de nos objectifs stratégiques tout au long de l'année.

INDICATEURS CLÉS DE PERFORMANCE		**Résultats au 31.12.2022**	**Objectif 2022**
ICP 1 Indicateur interne	Nombre d'initiatives, y compris les publications, en matière de veille technologique et visant à promouvoir les technologies destinées à améliorer le respect de la vie privée et la protection des données organisées ou coorganisées par le CEPD	13 initiatives	10 initiatives
ICP 2 Indicateur interne et externe	Nombre d'activités axées sur des solutions stratégiques interdisciplinaires (internes et externes)	8 activités	8 activités
ICP 3 Indicateur interne	Nombre de dossiers traités dans le cadre de la coopération internationale [Assemblée mondiale sur la protection de la vie privée, CdE, OCDE, GPEN, IWGDPT, conférence de printemps, organisations internationales] pour lesquels le CEPD a fourni une contribution écrite importante	27 dossiers	5 dossiers

ICP 4 Indicateur externe	Nombre de dossiers pour lesquels le CEPD a agi en qualité de rapporteur chef de file, de rapporteur ou de membre de l'équipe de rédaction dans le cadre du Comité européen de la protection des données	21 dossiers	5 dossiers
ICP 5 Indicateur externe	Nombre d'avis au titre de l'article 42 et d'avis conjoints du CEPD et du Comité européen de la protection des données émis en réponse aux demandes de consultation législative de la Commission européenne	4 avis conjoints 27 avis	L'année précédente en tant que référence
ICP 6 Indicateur externe	Nombre d'audits/visites effectués physiquement ou à distance	4 audits 2 visites	3 audits/visites différents
ICP 7 Indicateur externe	Nombre d'abonnés aux comptes de médias sociaux du CEPD YouTube (YT), LinkedIn (L), Twitter (T), EU Voice et EU Video	YT – 2,75k L – 63k T – 29,1k EU Voice – 5,1k EU Video – 0,69k	Résultats de l'année précédente + 10 %
ICP 8 Indicateur interne	Taux d'occupation du tableau des effectifs	86,9%	90%
ICP 9 Indicateur interne	Exécution du budget	98,2%	85%

edps.europa.eu

Office des publications
de l'Union européenne

EDPS