Université DPO 2025

Paris
6 & 7 février

Ouverture par Paul-Olivier Gibert, Président de l'AFCDP

C'est avec beaucoup de plaisir et d'émotion que je vous retrouve aujourd'hui pour cet événement devenu un rendez-vous incontournable pour les acteurs engagés dans la protection des données personnelles.

Nous allons explorer ensemble les défis et opportunités qui façonnent notre métier. Cette rencontre intervient à un moment clef : la protection des données personnelles est désormais un enjeu stratégique et un sujet central dans notre société. Ce n'est pas seulement une obligation légale, c'est une condition essentielle pour maintenir la confiance des citoyens dans la sauvegarde de leurs informations.
Le thème central de cette édition est la gouvernance des données à l'ère de l'intelligence artificielle.

Les défis sont nombreux : nous devons continuer à garantir le respect des réglementations tout en intégrant de nouvelles dispositions, comme celles de l'IA Act. Sur le plan éthique, il est primordial de surveiller l'évolution de ces technologies en veillant à respecter les principes de transparence, d'autonomie et d'équité. Comment faire en sorte que les algorithmes ne reproduisent pas nos biais ? C'est une question essentielle.
Plus de dix ans après la rédaction du RGPD, le rôle du DPO a profondément évolué. Il ne se limite plus à être un simple garant de la conformité : il doit désormais posséder une compréhension fine des technologies et une capacité à appréhender les métiers pour lesquels il travaille.

Cette Université ne se limite pas à ces deux journées. Nous avons mis en place un format hybride qui permet de les compléter par cinq sessions numériques. Nous avons conçu cet événement comme un parcours d'apprentissage continu, que nous continuerons d'enrichir au fil du temps.

Un élément important approche : le renouvellement du conseil d'administration lors de notre assemblée générale en juin prochain. C'est une étape clef pour définir l'avenir de l'AFCDP. Aujourd'hui, nous lançons un appel à candidatures : si vous souhaitez contribuer activement au développement de l'association, c'est l'occasion idéale de vous engager en tant qu'administrateur. J'invite chaleureusement ceux qui le souhaitent à déposer leur candidature. C'est un engagement essentiel pour faire vivre notre communauté.

En guise de bilan, ces quatre dernières années ont marqué un changement de dimension pour notre association. Nos dépenses pour 2024 ont atteint 1,4 million d'euros. L'activité a doublé : nous sommes passés de moins de 60 réunions en 2020 à 150 en 2024. Notre visibilité s'est également accrue, avec 245 retombées presse cette année. Nous sommes

très fréquemment consultés par les institutions lors de l'évolution des textes réglementaires, et nous avons renforcé nos relations avec d'autres organismes, notamment le Parlement et les instances exécutives.

Ainsi, devenir administrateur de l'AFCDP n'est pas un choix anodin. Il s'agit d'une association reconnue et suivie, une responsabilité à assumer pleinement.
Pour conclure, je tiens à vous remercier sincèrement. C'est un bonheur et un honneur de m'engager à votre service au sein de l'AFCDP.

Introduction de l'ANSSI par Emmanuel Naegelen, Directeur général adjoint

Merci pour cet honneur fait à l'Agence d'ouvrir cette Université. Je suis impressionné par la vitalité de cette association. Je dois avouer être un peu jaloux : j'aimerais réussir à fédérer les RSSI de la même manière, mais nous n'avons pas encore d'événement qui rassemble autant de monde dans une seule salle.

Je vais centrer mon intervention sur la question des données. En y réfléchissant, la donnée, dans le monde numérique, est une ressource abondante. Nous en générons constamment, en quantité croissante. Mais c'est aussi une ressource extrêmement convoitée par un grand nombre d'acteurs, qu'ils soient économiques ou criminels. Dans ce contexte où la donnée est omniprésente et toujours plus précieuse, comment parvenir à la protéger de manière proportionnée ? C'est une question clef pour l'ANSSI. Comment éviter une sous-protection ou une surprotection ? Comment assurer une cohérence entre le RGPD et les obligations de cybersécurité, notamment celles introduites par NIS 2 ? Être conforme au RGPD signifie-t-il être conforme à NIS 2 ? Et comment adapter notre protection à l'évolution des technologies, notamment à l'intelligence artificielle, qui soulève de nouvelles problématiques en matière de sécurité des données ?

Plutôt que de proposer un exposé théorique, j'adopterai une approche pragmatique, en lien avec mon parcours militaire. Je structurerai mon propos autour de deux axes :

1. Les enjeux pesant sur nos données
2. Les stratégies de protection à mettre en place

1. Les enjeux pesant sur nos données

Chaque année, nous publions notre « bestseller » : le panorama de la menace. L'édition 2024 paraîtra le 11 mars et même si je ne peux pas tout dévoiler avant sa sortie, je peux partager quelques tendances marquantes.

- L'exploitation des données volées évolue : traditionnellement utilisées pour des extorsions par des cybercriminels, elles sont de plus en plus exploitées à des fins de déstabilisation par des activistes.

- Lors des JO 2024, un groupe opposé à la participation d'Israël a revendiqué le vol de données du CNOSF. La réalité du vol a été confirmée, bien qu'il s'agisse de données issues de vieux sites web mal décommissionnés. Pourtant, l'impact médiatique a été significatif.

- Autre exemple : la divulgation par des groupes pro-russes de données issues de l'agence polonaise anti-dopage, visant à discréditer la lutte antidopage et à semer la désinformation.

- L'exploitation des prestataires informatiques et des infrastructures cloud :
  - De nombreuses fuites proviennent aujourd'hui des prestataires de services qui, disposant d'un accès privilégié aux systèmes d'information de leurs clients, deviennent des cibles de choix.
  - Les hyperviseurs, ces logiciels permettant de gérer un grand nombre de clients sur une infrastructure cloud, sont particulièrement vulnérables. Un attaquant qui compromet un hyperviseur peut discrètement accéder à de multiples clients.
- Le secteur social et les agences d'État sont des cibles privilégiées, notamment via les prestataires de tiers payant.
- Le marché noir des données sur le dark web se structure : malgré les opérations de police et les démantèlements de plateformes illégales, de nouveaux forums émergent rapidement.

Deux tendances fortes se dégagent :
1. Une menace industrialisée qui cible massivement les données, encouragée par une relative impunité malgré les efforts des services de police et de justice.
2. L'essor de l'hacktivisme dont l'impact sur les systèmes reste limité, mais qui peut provoquer des crises médiatiques majeures selon les données divulguées.

<u>2. Quelles stratégies pour protéger efficacement les données ?</u>
- Le droit est un outil puissant car il permet d'imposer des obligations aux acteurs critiques.
- Directive NIS2 : un chantier majeur
  - NIS2 va considérablement élargir le nombre d'entités régulées par l'ANSSI, passant de 400-500 entités actuellement à 15 000 - 20 000.
  - Une différence majeure avec le RGPD : alors que ce dernier est entré en vigueur avec des obligations générales, NIS 2 nécessite un référentiel d'exigences précises, en cours d'élaboration. Ce référentiel fera l'objet d'une consultation publique au second trimestre 2025.
  - Plusieurs services en ligne seront développés pour faciliter la mise en conformité :
    - Un outil pour tester son éligibilité à NIS2
    - Un portail pour s'enregistrer facilement comme entité régulée
    - Une plateforme de notification des incidents de cybersécurité
  - En matière de contrôle, une phase de montée en compétence est prévue : en 2026, des contrôles à blanc seront réalisés, mais les véritables contrôles ne commenceront pas avant trois ans.
  - Les bonnes pratiques techniques restent essentielles
    - L'ANSSI met à disposition une collection de guides pratiques.
    - Dernière publication en date : « 11 bonnes pratiques pour éviter les fuites de données » co-rédigée avec la CNIL et Cybermalveillance.gouv.fr.

J'espère avoir démontré la convergence entre cybersécurité et protection des données, qui se traduit par une coordination permanente entre l'ANSSI et la CNIL. Nous partageons les mêmes problématiques et cherchons ensemble des solutions communes.

Enfin, concernant les risques liés aux nouvelles technologies, je vous invite à suivre le sommet de l'IA, qui aura lieu lundi et mardi. L'ANSSI y est fortement impliquée et publiera à cette occasion une analyse des risques liés aux systèmes d'IA, co-signée par une quinzaine de pays, afin d'aider les utilisateurs d'IA à mieux évaluer leurs risques.
De nombreux débats sont en cours au niveau européen sur la question du cadre juridique applicable aux entreprises (siège social, établissement principal…). Ces sujets sont en cours d'instruction et nécessiteront des clarifications.

VIGINUM : comment protéger le débat public numérique dans le strict respect des libertés individuelles par Marc-Antoine Brillant, responsable VIGINUM, et Jean-Luc SAURON, Président du comité éthique et scientifique

Les raisons ayant conduit à la création d'une agence nationale dédiée tiennent au constat répété de la manipulation de l'information. On peut citer plusieurs événements marquants : les MacronLeaks, le mouvement des Gilets Jaunes avec des ingérences étrangères cherchant à attiser la colère, ou encore la crise du Covid-19 où de nombreuses opérations d'influence et de communication stratégique ont émergé.

En 2020, après l'assassinat de Samuel Paty, une vaste campagne anti-française s'est déployée sur les réseaux sociaux, ciblant notamment les intérêts économiques du pays. Face à ces constats, la nécessité d'une structure spécifique s'est imposée, et le décret du 13 juillet 2021 a officiellement créé VIGINUM. L'objectif était de définir clairement les menaces à traiter. Il ne s'agit pas de surveiller toutes les manipulations d'information, mais de se concentrer sur celles qui impliquent des États étrangers et qui visent les intérêts nationaux.

VIGINUM est un service opérationnel dédié à la détection et caractérisation des opérations d'ingérence numérique étrangère. Il analyse les données accessibles publiquement en croisant expertise géopolitique, OSINT et science des données. Son approche repose sur l'étude des modes opératoires et techniques de diffusion, plutôt que sur l'analyse de contenu.

Ce qui distingue VIGINUM, c'est son cadre juridique extrêmement strict. Un second décret du 7 décembre 2021 a encadré l'utilisation d'un traitement automatisé de données à caractère personnel dans le but d'identifier les ingérences numériques étrangères. L'innovation majeure a été l'introduction d'un comité éthique et scientifique, garantissant un contrôle rigoureux de l'activité du service.

Les menaces observées

1. Dissémination des manipulations d'information
    - Ces pratiques ne sont plus seulement limitées aux élections : elles concernent désormais l'ensemble des débats publics.
    - La principale tendance actuelle n'est plus tant la diffusion de fake news que l'instrumentalisation du vrai par des acteurs étrangers.
2. Sophistication des modes opératoires

    - On est passé des simples bots et trolls à des techniques plus avancées visant à manipuler les algorithmes des plateformes et à utiliser massivement l'IA générative.
3. Recours à des intermédiaires
    - Certains États utilisent des sous-traitants ou des prestataires privés pour mener des campagnes de manipulation.

VIGINUM a publié six rapports en 2023 documentant ces phénomènes et identifie trois profils d'acteurs impliqués :

- Acteurs persistants : bien positionnés dans le débat public, ils connaissent parfaitement les dynamiques françaises.
- Acteurs opportunistes : ils repèrent des thématiques sensibles et cherchent à les instrumentaliser.
- Acteurs périphériques : ils ciblent en priorité d'autres pays, mais la France peut être touchée indirectement.

Il est essentiel que VIGINUM puisse présenter son travail au public. La manipulation de l'information touche toute la société et nécessite une réponse collective.

Le Comité éthique et scientifique (CES) est composé de membres de l'ARCOM, de journalistes spécialisés en fact-checking, d'un diplomate, d'un magistrat judiciaire et d'autres experts. Le CES se réunit chaque mois et échange toutes les deux semaines avec VIGINUM pour assurer un suivi constant.

Trois axes de travail prioritaires

1. Juridique : adapter et renforcer le cadre légal.
2. Mobilisation de la société civile : sensibiliser les citoyens aux manipulations d'information.
3. Anticipation des menaces : étudier les tendances actuelles et futures (exemple : observation du débat en Allemagne).

La Réserve citoyenne numérique prévue par l'article 23 de la loi du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique sur la sécurité numérique permettra de mobiliser des citoyens pour surveiller les réseaux sociaux et signaler les contenus illicites au Parquet.

Un enjeu majeur est l'européanisation de la réponse. En juillet 2024, la présidente de la Commission européenne a évoqué la création d'un *VIGINUM européen*. Si le modèle exact reste à définir, le modèle français est cité en référence dans les conclusions du Conseil européen.

Auditer un système d'IA en production : défis et retours d'expérience par Benoit Rottembourg, auditeur à l'INRIA

Il y a cinq ans, nous avons rencontré un paradoxe avec ma direction : nous avions beaucoup contribué à la fabrication d'algorithmes, mais nous avions moins participé à leur vérification. C'est pour cette raison que nous avons développé Regalia. Mon objectif aujourd'hui est de vous faire prendre conscience des biais existants, de leur nature, des

types de problèmes qu'ils engendrent et des raisons pour lesquelles ils apparaissent. Je vous propose de vous mettre, pendant quelques minutes, dans la peau d'un auditeur.

Pour illustrer mon propos, voici une anecdote datant de 1998. J'avais développé une intelligence artificielle chargée de planifier les emplois du temps de centaines de milliers de conseillers clientèle. Un soir, un syndicat de centre d'appel m'a contacté pour signaler une injustice : les personnes en fin d'alphabet subissaient des emplois du temps bien plus dégradés que celles en début d'alphabet. Ma première réaction a été de me défendre en expliquant que je ne disposais pas des noms des agents et que cela ne pouvait donc pas être ma faute. Pourtant, cette réflexion m'a travaillé, et j'ai fini par comprendre que les identifiants des agents étaient reçus dans l'ordre alphabétique sans que je le sache.
Mon logiciel, en optimisant les plannings, surchargeait la fin de la liste et attribuait les shifts les plus défavorables aux derniers agents. La correction de ce biais n'a nécessité qu'une simple ligne de code. Cet exemple montre que les biais ne sont pas toujours intentionnels et qu'ils peuvent prendre des formes inattendues. Réparer un algorithme ne signifie pas le détruire.

Pourquoi le coupable idéal n'existe pas ?
Plusieurs raisons expliquent pourquoi les algorithmes dérapent ou sont mal utilisés. Tout commence par leur conception. Les algorithmes développent souvent un « talent par proxy » : ils optimisent en fonction de critères indirects qui ne sont pas toujours explicitement prévus.

Les normes métriques ne sont pas encore bien définies. On peut vouloir que les résultats d'un algorithme soient statistiquement équivalents entre hommes et femmes, mais les performances peuvent tout de même varier. La notion de biais individuel est donc très difficile à définir.

Pour surveiller les algorithmes et éviter les dérives amplifiées par les données, certaines exigences doivent être posées : à commencer par la question cruciale « Avez-vous utilisé la bonne IA ? » Toutefois, ce constat arrive souvent trop tard, alors que de nombreux domaines comme le e-commerce reposent déjà sur ces algorithmes.

L'audit comportemental
Aujourd'hui, nous ne pouvons plus simplement comprendre le code source d'un algorithme. Nous devons analyser son comportement en observant ses résultats, comme si nous secouions une « boîte noire » pour voir ce qui en sort. Cet audit comportemental nécessite une bonne connaissance du domaine et un accès à des données de qualité afin de dégager des conclusions probantes.
Prenons l'exemple du recouvrement d'impayés : un centre d'appel applique des règles métier, mais de plus en plus, des algorithmes sont utilisés pour scorer la probabilité qu'une personne ne paie pas sa facture. Ce scoring repose sur des données comme l'âge, le genre ou la localisation géographique, exploitées à partir de statistiques portant sur un million de dossiers.

L'algorithme peut alors amplifier localement certains biais, créant des zones de préjudice réel, notamment dans des secteurs à haut risque tels que le recrutement, le crédit ou la

médecine. Il est donc essentiel d'aller au-delà de la data science et d'impliquer les experts métiers dans ces audits.

Il est important de mettre en place, au sein des entreprises, des mécanismes permettant aux auditeurs, aux experts métiers et aux concepteurs d'algorithmes de collaborer. Détecter un biais de manière isolée est rare : si l'on se contente d'analyser des données sous Excel sans recul, il est facile de tirer des conclusions erronées. Par ailleurs, il faut faire attention aux intervalles de confiance : détecter un biais alors qu'il n'y en a pas peut induire en erreur. L'essentiel est de vérifier que le biais identifié a un préjudice réel sur la population concernée.

Enfin, les effets indésirables doivent être collectés, à l'image des notices médicales qui listent les effets secondaires d'un médicament. Parfois, un algorithme est simplement utilisé dans un mauvais contexte. Il est important de noter que corriger ces biais ne coûte pas forcément cher. Il ne s'agit pas d'opposer innovation et sécurisation des systèmes d'IA mais de les allier. Bien souvent, les data scientists sont sous pression de la part des métiers et ne prennent pas le temps nécessaire pour bien faire leur travail.
En conclusion, auditer un système d'IA est un exercice nécessaire, qui requiert un regard méthodique et multidisciplinaire pour assurer à la fois performance et équité.

OSINT : que peut apporter au DPO la maîtrise des technologies de renseignement en source ouvertes par Valentin Thévenot, DPO Interne & Chargé de sécurité du SI

L'OSINT, qui signifie Open Source Intelligence, se traduit par ROSO (Renseignement en Sources Ouvertes) : il s'agit de collecter des données dans le but d'obtenir de l'information. Quelles données sont concernées ? Ce sont des données brutes, sans valeur à proprement parler, l'important est que ces données soient accessibles à tous. Elles peuvent être mises à disposition par des particuliers, des entreprises ou des administrations.

L'enjeu majeur réside dans le fait qu'on ne peut pas collecter et analyser n'importe quelle donnée. L'objectif est d'en extraire de l'information exploitable. Si ces données concernent des individus, elles doivent respecter le RGPD. Une deuxième règle est qu'accéder à un système d'information et s'y maintenir constitue un délit. Un site mal sécurisé ne signifie pas que ses informations sont publiques. De plus, il est interdit de télécharger un leak de données en dehors du cadre du RIFI. Pour garantir que les données sont collectées et utilisées de manière conforme, il est essentiel de tout documenter.

L'OSINT repose sur un postulat : quelles sont les données qui existent sur moi sur Internet ? Cette méthode est utilisée par des journalistes d'investigation, des services de renseignement, des chercheurs en généalogie, ou encore dans l'intelligence économique. Elle peut être exploitée à des fins malveillantes, comme dans le cas de cambriolages, de violences sexuelles ou de cyber-reconnaissance. La CNIL s'intéresse d'ailleurs à ce sujet, notamment via la question du recoupement d'informations en ligne.

L'OSINT n'est pas un monolithe, il existe plusieurs types : IMINT, GEOINT, SOCMINT, GOOGLINT. N'importe qui peut pratiquer l'OSINT, un exemple en est la recherche d'image inversée sur Google ou l'analyse des métadonnées d'images.

Owen Mundy a par exemple réalisé une cartographie des photos de chats en ligne. Un autre exemple est le StravaLeaks (avec des informations sur des joggings, ou la localisation du président). Les lunettes Meta sont aussi un cas intéressant d'utilisation de l'OSINT.

Le rôle du DPO est de poser les critères de l'éthique : jusqu'où peut-on aller dans l'intimité des personnes ? Tout en comprenant le besoin, il doit établir un cadre. Il peut aussi être force de proposition dans la réidentification des personnes.

Vidéosurveillance et IA : garantir la conformité au RGPD pour protéger les libertés publiques par Alexandra ADERNO & David CONERARDY, avocats

L'objectif est de comprendre leur cadre légal et réglementaire y compris les implications du RGPD et de la loi JOP 2024. Il s'agit également d'identifier les risques juridiques et éthiques associés aux dispositifs de caméras augmentées et de maîtriser les étapes pratiques pour garantir la conformité légale et organisationnelle.

- **Vidéosurveillance** : dispositifs non ouverts au public.
- **Vidéoprotection** : dispositifs situés dans des lieux publics ou ouverts au public, régulés par le Code de la sécurité intérieure. Lors de la loi LOPSI 2, le Conseil constitutionnel a clarifié la qualification de la vidéosurveillance. Tout ce qui concerne des missions de vidéosurveillance relève du pouvoir de police administrative générale inhérent à la force publique.
- Les **caméras augmentées** intègrent des logiciels d'analyse algorithmique permettant de détecter des événements spécifiques, tels que des objets abandonnés ou des mouvements inhabituels, avec des fonctionnalités en temps réel. Leur finalité n'est pas l'identification unique d'une personne. Contrairement à la simple vidéosurveillance, les caméras augmentées ne se contentent pas de filmer la personne, elles analysent aussi automatiquement pour collecter des informations. Ces caméras ne sont pas synonymes d'analyse automatique des images en temps réel, cette dernière étant utilisée pour des recherches a posteriori, notamment dans le cadre du Code de procédure pénale.
- Les **caméras biométriques** utilisent des techniques informatiques pour reconnaître un individu à partir de ses caractéristiques physiques ou comportementales.

Loi JOP et décret JOP

Les finalités de cette loi sont de garantir la sécurité des manifestations sportives, culturelles et récréatives à forte affluence, en permettant la détection en temps réel d'événements prédéfinis susceptibles de présenter des risques pour la sécurité. Les acteurs autorisés à intervenir sont les services de police nationale et gendarmerie, ainsi que les services internes de sécurité de la SNCF et de la RATP.

Ce dispositif reste en application à titre expérimental jusqu'au 31 mars 2025, avec une possible pérennisation. Cependant, le bilan est assez mitigé. Le cadre juridique de la loi JOP est extrêmement restrictif. Par exemple, lorsqu'elle est saisie par des collectivités territoriales (CT) ou des bailleurs sociaux, elle est souvent perçue comme une opportunité de déployer des systèmes de vidéoprotection sur l'espace public. Or, en étudiant de plus près la loi JOP, on constate que ses applications sont très strictement encadrées. Les auteurs et finalités sont précisément définis, et les collectivités locales n'ont pas la possibilité de l'appliquer librement. Le traitement des données ne peut pas être continu ; l'outil ne doit permettre que la détection d'événements prédéterminés, susceptibles de révéler des actes de terrorisme, avant de saisir les forces de l'ordre pour intervention. Nous parlons bien ici de caméras augmentées, et non de caméras biométriques ou de reconnaissance faciale. Le traitement des données ne doit pas aboutir à des décisions individuelles.

Le décret associé a précisé ces restrictions en énumérant de manière exhaustive et limitative les événements pouvant faire l'objet d'analyses algorithmiques.
Un rapport du comité d'évaluation est mitigé. Bien que la loi JOP et son article 10 aient suscité beaucoup d'attentes, les caméras augmentées n'ont pas été largement utilisées, en raison notamment de la mobilisation des forces de police et de la faible maturité technologique des dispositifs. Le risque d'erreur reste élevé (ex : faisceau de lumière détectant un incendie ou des personnes statiques associés à des objets). Il existe aussi un temps nécessaire pour la formation, le calibrage, et le paramétrage des systèmes.

Il persiste un flou juridique quant au régime applicable aux caméras augmentées dans les lieux publics, qu'elles soient utilisées à des fins de police administrative ou judiciaire.

Le logiciel Briefcam a été au centre de plusieurs requêtes en référé-liberté déposées par des associations en novembre 2023 contre l'utilisation de ces dispositifs. Le Tribunal administratif de Lille (29 novembre 2023, n°2310103) a jugé qu'il n'y avait pas de caméras biométriques, mais uniquement des caméras augmentées sur réquisition judiciaire et en différé. De plus, l'usage ne permet pas l'identification des personnes et n'est pas considéré comme un traitement de données personnelles. À Nice, dans une autre décision du 29 novembre 2023 (n°2305692), le juge a demandé à la Ligue des droits de l'Homme de prouver le mésusage par la commune des outils de reconnaissance faciale. Le juge a interdit la reconnaissance faciale, mais a validé l'utilisation des caméras augmentées, en soulignant que ces dernières ne sont pas identifiantes et ne portent pas atteinte aux droits et libertés fondamentales. Actuellement, si vous utilisez des caméras augmentées, vous êtes en règle.
À Grenoble, le tribunal a repris les dispositions de la CNIL. Le flou juridique persiste, et les administrations ne sont pas homogènes dans leurs pratiques. Il n'y a pas encore de loi claire sur les caméras augmentées, et qu'en est-il de la vidéosurveillance professionnelle ? Selon une communication de la CNIL en novembre 2024, elle a estimé qu'il n'est pas nécessaire de disposer d'une loi spécifique pour des cas comme le transport de marchandises, où l'intérêt légitime peut être invoqué. Mais pour la vidéosurveillance professionnelle, qu'est-ce qui empêche l'usage des caméras augmentées ?

La loi JOP a créé un précédent dans les collectivités territoriales, et la question se pose de savoir si l'entrée en vigueur de l'IA Act pourrait engendrer une nouvelle émulation. Bien qu'il n'existe pas encore de base législative pour autoriser son usage, il y a un texte pour encadrer les risques liés aux caméras augmentées. Pourquoi ne pas envisager que l'IA Act serve de base à ce cadre juridique ?

Je n'ai plus d'outil spécifique pour mon registre, et c'est très bien comme ça par Jacques-Olivier Fabre, DPO de la ville de Narbonne

L'objectif est de simplifier la gestion en utilisant des outils bien connus des référents.
Pourquoi avoir initialement choisi une application adaptée au traitement du RGPD ? L'application a été choisie pour la reconnaissance de la société éditrice, l'avantage de sa granularité très fine, ainsi que la formation spécifique à destination des référents. Elle permet une démonstration rapide de la création d'un registre conforme à la CNIL, tout en facilitant les relations avec les référents et la gestion des PIA (Projets d'Impact sur la Vie Privée).

Inconvénients :

- Complexité à renseigner le registre, notamment pour les activités de traitement avec plusieurs finalités, bases légales et durées de conservation différentes.
- Formation des agents trop longue et complexe pour un usage finalement peu fréquent une fois les fiches de registre créées.
- Navigation dans les fiches du registre trop complexe, avec trop d'écrans à consulter.
- Edition trop lourde des fiches, qui peuvent s'étendre sur plusieurs pages même pour les plus simples.
- Rigidité de la solution et doutes sur l'accountability.

Formation des référents :
La formation est divisée en trois parties : une introduction, un outil spécifique et une fiche de registre, avec un focus particulier sur les mesures de sécurité. Cette formation est simplifiée autant que possible et s'appuie sur un modèle proche de celui de la CNIL. Un système de « navette » est utilisé pour les mesures de sécurité qui ne sont disponibles qu'en visualisation sur le serveur.

Bilan de la démarche :
Cette procédure a considérablement simplifié la gestion du RGPD, réduisant ainsi le temps et les efforts nécessaires à la gestion des registres et à l'interaction avec les services. Les référents ont constaté une nette amélioration dans la compréhension de la gestion de leurs données par rapport à l'application initiale, notamment grâce à des applications bureautiques familières, faciles à utiliser et offrant une plus grande autonomie.

Cela permet également une meilleure réactivité aux demandes de mises à jour et de modifications, tout en étant en mesure de faire face aux réorganisations fréquentes des services et aux changements de référents grâce à une formation simple et rapide, accessible à tous les niveaux.

Intervention de la CNIL par Louis Dutheillet de Lamothe, Secrétaire général

Je vais structurer mon intervention autour de trois axes principaux :

1. Un bilan général, comprenant des éléments inédits du rapport annuel ainsi que des données chiffrées.
2. Un point sur les outils mis en place par la CNIL pour diffuser sa doctrine et les projets en cours.
3. Une réflexion sur l'intelligence artificielle, notre vision sur le sujet, les prochaines publications et, le cas échéant, la question des applications mobiles.

1. Bilan général et évolution des activités de la CNIL

L'année 2024 est une bonne année pour la CNIL, malgré quelques turbulences budgétaires (une réduction de 10 % sur un budget de 4 millions d'euros). On dit souvent que la CNIL fonctionne sur deux jambes : son rôle de contrôle et de sanction, mais aussi son rôle d'accompagnement.

Concernant les plaintes, les contrôles et les sanctions, nous constatons une augmentation continue. Lors de l'adoption du RGPD en 2016, nous recevions environ 7300 plaintes. En 2024, ce chiffre est monté à 17000, ce qui représente un enjeu considérable pour nos services. Depuis plusieurs années, la Présidente de la CNIL a fixé l'objectif de traiter 100 % des plaintes. Certaines sont résolues rapidement, tandis que d'autres donnent lieu à des contrôles approfondis.

L'activité de contrôle s'est maintenue, mais le nombre de mesures correctrices a fortement augmenté. En 2024, nous avons pris 331 mesures correctrices, contre seulement 55 il y a quatre ans et demi, soit une multiplication par six. Cette hausse répond aux attentes des DPO, qui souhaitent une action plus crédible de la CNIL. Par le passé, nous avions pris des sanctions importantes contre quelques grands acteurs, mais il était nécessaire d'étendre cette démarche.

En 2024, nous avons prononcé 87 amendes, dont 18 selon la procédure ordinaire. La procédure simplifiée a pris de l'ampleur, avec 87 sanctions l'an dernier. Nous avons émis 180 mises en demeure et plus de 60 rappels aux obligations légales signés par la Présidente.

Pour l'année à venir, nos actions de contrôle se concentreront sur deux domaines déjà annoncés : les applications mobiles et la sécurité des données. L'année 2024 a été marquée par de nombreuses cyberattaques et violations de données. Beaucoup d'attaques auraient pu être évitées en appliquant les recommandations de la CNIL et de l'ANSSI. Nous allons donc renforcer notre action pour en tirer les conséquences et améliorer la sécurité des données.

2. Outils et accompagnement des DPO

La CNIL s'efforce de répondre aux attentes des DPO et des responsables de traitement. Nous avons reçu 6600 appels dans nos permanences et organisé plusieurs journées d'échange en région.

Une étude récente, menée avec l'AFCDP et le ministère du Travail, met en avant la diversité croissante des profils des DPO. Ce rôle n'est plus uniquement occupé par des juristes, en raison de l'explosion des textes réglementaires sur les données et les technologies numériques. Toutefois, une tendance inquiétante émerge : en 2019, 27 % des DPO se déclaraient peu ou pas formés ; en 2024, ce chiffre a bondi à 55 %. Beaucoup estiment ne pas avoir assez de ressources pour se tenir informés.

Pour y remédier, la CNIL va créer en 2025 un **kit d'embarquement** pour les nouveaux DPO. Chaque nouveau délégué bénéficiera d'un ensemble de ressources adaptées : documents simples et accessibles, mais aussi contenus plus techniques pour répondre aux questions juridiques spécifiques. En parallèle, la CNIL enverra un courrier aux responsables de traitement pour leur rappeler le rôle du DPO et ses garanties, afin de mieux intégrer ce dernier dans la gouvernance de l'entreprise.

Par ailleurs, je rappelle l'existence de la Table Informatique & Libertés. Mise à jour tous les deux ou trois mois, elle répertorie les positions prises par la CNIL sur divers sujets. Un exemple récent concerne un système de géolocalisation qui fonctionnait en dehors des horaires de travail d'un salarié. Nous avons jugé qu'il n'était pas proportionné et avons rappelé l'interdiction de suivre un véhicule professionnel lorsque l'employé est autorisé à l'utiliser à titre privé.

3. Intelligence artificielle et protection des données
L'IA est un sujet central. La CNIL a lancé un plan spécifique visant les concepteurs d'IA. Nous devons permettre aux entreprises européennes de développer des modèles de langage et d'analyse automatique, tout en respectant la réglementation sur la protection des données.
Deux recommandations de la CNIL seront bientôt publiées :

1. La manière d'informer les personnes dont les données sont traitées par une IA.
2. La question du traitement des demandes d'exercice de droits dans un contexte d'IA.

La maîtrise technologique, un outil efficace pour la SSI par Jean-Séverin Lair, DSI au sein de l'INSEE

Nous manipulons un volume colossal d'informations à l'INSEE avec des éléments sensibles comme le NIR et ou d'importants volumes tels que le recensement de la population. Dans ce contexte, la maîtrise technologique est essentielle et doit primer sur le discours commercial.

La maîtrise technologique : une nécessité face aux solutions commerciales
Une technologie n'est pas une solution en soi. Elle repose sur un ensemble de techniques, de connaissances et d'outils permettant de répondre à des besoins. Or, les commerciaux cherchent souvent à nous convaincre qu'une technologie est une solution clef en main.

Un élément essentiel à garder en tête est l'effet Dunning-Kruger qui met en évidence un biais cognitif selon lequel nous avons tendance à surestimer notre compétence dans un domaine lorsque nous commençons à l'explorer. La véritable maîtrise technologique

permet d'éviter la dépendance aux solutions commerciales qui présentent des risques budgétaires et sécuritaires. Lorsque nous nous appuyons sur des boîtes noires, nous limitons notre capacité d'analyse et de sécurisation.

Il est crucial de comprendre que le cloud ne se résume pas à des fournisseurs comme Amazon ou Google. Le cloud repose sur des technologies précises : virtualisation, conteneurisation, stockage objet, etc. La maîtrise de ces technologies est essentielle pour assurer leur mise en œuvre sécurisée.

Nous avons adopté une approche en deux axes :

- Renforcement des compétences internes : nous avons mis en place une infrastructure basée sur des solutions open source (vanilla) afin de comprendre les fondements de ces technologies.
- Développement d'une infrastructure spécifique pour la data science avec la souche Onyxia, afin d'approfondir notre expertise.

Maîtriser la complexité des développements

Le développement informatique est un domaine en constante évolution. Plus les langages, frameworks et bibliothèques se multiplient, plus le maintien en condition de sécurité devient complexe. Il est donc essentiel de trouver un équilibre entre innovation et maîtrise de l'environnement technique.

À l'INSEE, nous avons longtemps utilisé JAVA et SaS comme principaux langages. Aujourd'hui, nous avons élargi notre champ avec Python, en veillant à faire des choix technologiques rationnels. Un autre point essentiel est la gestion des bibliothèques utilisées dans nos développements. Nous demandons aux développeurs de prendre en compte les dépendances et de corriger les failles de sécurité identifiées dans les bibliothèques externes qu'ils intègrent. Par ailleurs, une mauvaise approche de la sécurité applicative peut créer plus de vulnérabilités qu'elle n'en résout. Il est donc primordial de ne pas se fier à des solutions miracles et de rester vigilant face aux promesses commerciales.

Les outils collaboratifs (intranet, messagerie, visio-conférence) sont souvent gérés par les services de communication interne qui font appel à des solutions externes sans forcément prendre en compte les enjeux de sécurité et de protection des données. Pourtant, ces outils sont essentiels dans l'activité quotidienne et nécessitent une vigilance particulière notamment avec l'émergence de l'intelligence artificielle.

Développer les compétences internes pour garantir la maîtrise technologique

Une stratégie efficace repose sur des compétences internes solides. Une approche intéressante consiste à collaborer avec des petites structures capables de mobiliser des experts en fonction des besoins.

La maîtrise technologique et l'innovation doivent aller de pair. Toutefois, l'innovation ne doit pas être systématiquement synonyme de complexité accrue ou de risques supplémentaires pour la sécurité des systèmes d'information et la protection des données. À l'INSEE, nous avons mis en place une division dédiée à l'instruction technique et à l'innovation. Nous avons notamment travaillé sur un projet d'open data conçu dès le départ sans contraintes de sécurité particulières (puisque les données étaient ouvertes). Par la suite, ce projet a été enrichi et sécurisé pour devenir une solution

interne robuste. Cette approche nous a permis de concilier innovation et exigences de sécurité.

Conclusion

Pour garantir une bonne sécurité des systèmes d'information, la maîtrise technologique est essentielle. Il ne s'agit pas seulement de dépasser le discours commercial, mais aussi de comprendre les technologies sous-jacentes, de développer les compétences internes et de laisser la place aux talents. C'est en dépassant les solutions toutes faites que nous pouvons véritablement assurer la sécurité et l'efficacité de nos systèmes.

Merci pour votre lecture !

Sylvain CHEMTOB
Président I Phénix Privacy

Port : +33 7 44 96 20 16
Fixe : +33 4 22 91 42 56
direction@phenix-privacy.com
93, rue de la Part-Dieu
69003 Lyon
www.phenix-privacy.com

PHENIX PRIVACY
Notre expertise privacy à votre service
93, rue de la Part-Dieu
69003 Lyon
+ 33 7 44 96 20 16
www.phenix-privacy.com