



Journée CNIL Montpellier 4 décembre 2024



Aujourd'hui Phénix Privacy vous emmène à Montpellier pour rencontrer la Commission Nationale Informatique et Libertés.

Dès 2022, la CNIL a lancé une série de rencontres avec les professionnels à travers la France, et après Lyon, Nancy, Lille, Toulouse, Marseille et Rennes, c'est au tour de Montpellier.

Cette journée d'échange s'est déroulée à l'Institut de Botanique de Montpellier – un des sept instituts universitaires de Montpellier, université fondée en 1289 – et ça tombe bien car chez Phénix Privacy, les plantes c'est notre passion !

Dans l'Hérault, la CNIL a vu les choses en grand ! Au-delà de cette journée de sensibilisation, quatre journées supplémentaires sont consacrées à des rencontres pour informer le public sur le numérique et ses droits. Au programme : ateliers, interventions en classe, et cafés des parents, spécialement conçus pour expliquer à chacun, petits et grands, comment protéger ses données personnelles et sa vie privée.

Revenons à notre journée dédiée aux professionnels avec un programme costaud couvrant des thématiques qui intéressent tout particulièrement les responsables RGPD, DPO et RSSI.

Voici le résumé des échanges rédigés 100 % par votre serviteur.

Ouverture

Lancement par Philippe AUGÉ, président de l'université de Montpellier qui introduit chaleureusement la journée. Par la suite, Marie-Christine SORDINO, vice-présidente déléguée à l'éthique et à la déontologie de l'université de Montpellier, rappelle les enjeux et risques propres à la réglementation et la décision de la [CJUE du 4 octobre 2024](#) sur les avantages indus par un non-respect de la réglementation en matière de concurrence. Pour marquer l'évolution des pratiques au sein de l'Université, elle évoque aussi l'évolution des pratiques de publication des notes des étudiants telle que la fin de l'affichage public des résultats et le choix d'une communication individualisée.

Puis Laurence FRANCESCHINI, commissaire de la CNIL et conseillère d'État, rappelle la volonté de la CNIL de multiplier les échanges en province dès 2022. Elle enchaîne sur un rapport d'étonnement sur la CNIL avec le [collège de la CNIL](#), composé de 18 membres venant d'horizon divers et notamment de la Cour des comptes et du Conseil d'État, la diversité des sujets abordés dont l'avis rendu pour la vérification de l'âge concernant les contenus pornographiques. La commissaire mentionne également le lien entre l'accompagnement de la CNIL, qui prépare l'avenir, et son contrôle, qui adresse le passé. Également, l'accompagnement de l'innovation dont la mise à disposition de bac à sable pour des projets soutenus. Enfin, elle souligne que l'innovation n'est pas incompatible avec le respect des droits fondamentaux et cite les [12 fiches pratiques sur l'IA](#) disponibles sur le site.

Marc SZTULMAN, conseiller régional d'Occitanie au numérique et président de Cyber'Occ, insiste lui sur les garde-fous mis en place pour limiter l'usage des données des citoyens européens dans le cadre de l'entraînement des grands modèles de langage nécessaires à l'IA.

Nicolas SAMARCQ, administrateur de l'AFCDP, rappelle quant à lui le doublement du budget de la CNIL en 2004 – lors de la transposition de la Directive de 1995 ancêtre du RGPD – et présente en détails les résultats du baromètre mesurant la confiance des DPO dans la mise en œuvre de la NIS 2 dans lequel seuls 13 % des répondants se disent « confiants ».

Manu REYNAUD, élu Ville Numérique à la métropole de Montpellier, qui est la seule ville ayant pris une délibération interdisant l'usage de la reconnaissance faciale dans le cadre de la vidéoprotection et l'interdiction de ChatGPT pour les agents de la ville, reprend les engagements de la ville en ce qui concerne l'usage de l'intelligence artificielle.

Session 1 - Les actualités

Éric DELISLE, chef du service des affaires sociales, des collectivités locales et de l'environnement à la CNIL, explique les réorganisations en cours au sein de la commission et présente les recommandations émises sur les enquêtes de mesure de la diversité au sein d'organismes publics et privés.

Il est rappelé que la mesure de la diversité au travail est possible en tenant compte des interdictions édictées par le Conseil constitutionnel dont l'impossibilité d'utiliser des critères sur l'origine ou la race ([Décision n° 2007-557 DC du 15 novembre 2007](#) : « si les traitements nécessaires à la conduite des études sur la mesure de la diversité des origines peuvent porter sur des données objectives, ils ne sauraient reposer sur l'origine ethnique ou la race »). Il reprend ensuite les obligations de la réglementation (finalité légitime, limitation des informations collectées, consentement, information des personnes...) et les recommandations dont le fait de privilégier l'anonymat, le recours à un tiers de confiance et la nécessité de réaliser une AIPD. Il est ainsi possible, sous-réserve de respect de la réglementation, de collecter des informations propres à la nationalité des parents, du ressenti d'appartenance pour mieux adresser les questions de diversité au travail (pour aller plus loin : [le projet de recommandation de la CNIL](#)).

Irène BAUDU, juriste au service de l'économie numérique et du secteur financier et Benjamin POILVÉ, ingénieur au service de l'expertise technologique à la CNIL, ont ensuite présenté les recommandations pour [une bonne maîtrise des smartphones](#). Parent pauvre de la conformité, l'encadrement des smartphones y est parfois négligé. Il est rappelé la nécessité de concevoir des applications qui respectent nativement la réglementation et de maîtriser l'intégration des outils tiers dans le développement des applications (évaluation préalable, qualification juridique, contractualisation, etc.). Une application mobile intègre en moyenne 15 SDK !

Astuce : le site [Exodus Privacy](#) permet de visualiser rapidement les SDK sollicités par une application mobile.

Session 2 – DPO au quotidien : les bonnes pratiques

Andrea MARTELLETTI, consultant RGPD et cybersécurité, rappelle utilement que le RGPD est là pour protéger les personnes des nuisances liées aux traitements de données. Le rôle du DPO, qui « ne doit pas être une tête à claque », l'oblige à s'adapter aux métiers en favorisant la mise en place de choses simples tout en priorisant ses actions en fonction des risques des traitements. Comme un trait d'humour, il évoque les risques sur « l'échelle du craignos » afin de mieux prioriser les actions portées par le DPO.

Jean-François MANGIN, DPO de la région Occitanie, voit le DPO comme un levier pour identifier des opportunités et des synergies avec une dynamique vertueuse basée sur le collectif. Il présente « les alliés » du DPO : RSE, Souveraineté digitale, IA, gouvernance des données, acculturation cyber/RGPD, souveraineté, cybersécurité...

Léah PEREZ et Nadia FORT, docteures en droit public et consultantes RGPD, nous parlent alors des analyses d'impact relative à la protection des données (AIPD) en partageant avec le public des recommandations :

- **Adopter une approche pragmatique** : éviter l'excès de zèle, hiérarchiser les AIPD entre elles et les prioriser en tenant compte des autres actions de conformité, et lancer la démarche au moment opportun ;
- **Impliquer les métiers** : adapter le message et utiliser les bons leviers selon ses interlocuteurs pour présenter efficacement la démarche ;
- **Délimiter clairement le périmètre** : définir les contours du projet et communiquer cette vision aux équipes concernées ;
- **Structurer la démarche en plusieurs étapes** : planifier par phases (lancement, ateliers espacés, validation des comptes-rendus), rédiger un rapport synthétique et organiser une restitution claire ;
- **Associer les sous-traitants** : les impliquer dès le départ pour garantir une cohérence dans l'approche ;
- **Privilégier la cohérence à l'exhaustivité** : il ne s'agit pas de tout décrire, mais de se concentrer sur les risques principaux, en se basant sur des scénarios crédibles et pertinents ;
- **Assumer son positionnement en tant que DPO** : veiller à impliquer les métiers et la direction dans la démarche ;
- **Gérer le syndrome de l'imposteur** : pour les juristes face aux aspects techniques, s'appuyer sur les ressources documentaires comme celles de la CNIL ou de l'ANSSI, étudier des exemples de traitements similaires pour s'inspirer, ne pas hésiter à solliciter un expert sans se sentir diminué ;
- **Maintenir le cap de la protection des droits fondamentaux et domestiquer la subjectivité** en croisant les points de vue et les expertises.

Session 3 – La gestion des plaintes

Nicolas MEIGNAN, délégué à la protection des données chez France Travail et Sophie GENVRESSE, cheffe du service de l'exercice des droits et des plaintes à la CNIL, évoque la plainte, « de l'occasion manquée à l'opportunité ».

Sophie constate la montée en compétence des personnes concernées avec beaucoup de plaintes pour des faits de tous les jours très souvent en lien avec l'exercice de leurs droits. Cela représente un doublement des plaintes depuis 2017 en passant de 8 000 à plus de 16 000 par an, prises en charge par une quarantaine de personnes dont 3 personnes chargées de vérifier leur recevabilité sur environ 300 agents en tout à la CNIL. Un service d'action rapide est en place pour traiter plus facilement les demandes avec une priorisation donnée aux situations des personnes concernées et à la capacité de la CNIL à débloquer les sujets avec le Responsable de traitement. La CNIL s'adresse aux DPO pour traiter les plaintes avec la possibilité de faire passer des messages et d'adresser conjointement des problématiques organisationnelles.

Nicolas évoque la montée des exigences et récriminations qui, sans retour favorable, donnent lieu parfois à une plainte auprès de la CNIL. France Travail a ainsi reçu plus de 4000 exercices de droits en 2024 avec évolution de l'organisation avec des équipes en région.

Pour Sophie, les plaintes permettent aussi de « faire évoluer des pratiques » telles les demandes d'effacement ont fait évoluer les pratiques journalistiques de citations des personnes impliquées

dans des accidents de la route et les demande de dé référencement qui sont mieux pris en charge par les moteurs de recherche.

Session 4 – La gestion des risques cyber

Florent DELLA VALLE, chef du service de l'expertise technologique à la CNIL, nous présente les actualités SSI. Il commence par rappeler que la protection des personnes physiques passe par la mise en place de mesures basiques en matière de protection des données (voir [guide de la sécurité des données personnelles](#)) telles que les mesures de protection découlant des AIPD et la notification des failles de sécurité en fonction de l'impact possible pour les personnes concernées. Il constate des violations de grande ampleur de plus en plus fréquentes avec la nécessité d'augmenter la sécurité pour ces traitements. Il est à noter que 55% des violations sont liées à des actes malveillants externes, 20% à des erreurs humaines internes et 25% à des causes autres dont la perte et le vol de matériel.

Enfin Marc SZTULMAN revient nous partager le constat d'un report des activités criminelles sur les cyberattaques qui sont plus lucratives et moins risquées au niveau pénal. À titre de comparaison, le ROI de la vente de faux médicaments est un multiple de 35, 32 pour la traite d'être humain avec un risque pénal élevé alors que les attaques cyber avec un multiple de 50 et un risque pénal moins forts seraient plus attractifs pour les criminels. Il appelle donc à une prise de conscience de la part de tous pour retrouver une nouvelle culture de la donnée avec du bon sens et moins de naïveté, une sorte de « paranoïa » de la donnée afin de développer une capacité collective à mieux adresser la gestion de la donnée et sa sécurisation.

C'est ainsi que cette intervention conclue une journée riche en échanges au sein du cadre verdoyant de l'Institut de Botanique de Montpellier !

Merci pour votre lecture !

Sylvain CHEMTOB
Directeur Général

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