



Faites de votre conformité un atout business !



Aspects juridiques du contexte du nouveau modèle de travail

François Coupez

Avocat à la Cour, associé

Certifié spécialiste Droit des nouvelles technologies (CNB), DPO (CNIL - AFNOR), ISO 27001
Lead Implementer et ISO 27701 Lead Implementer niveaux avancés (LSTI)

Chargé d'enseignements : Paris II Panthéon-Assas, CNAM, Paris-Dauphine



Colloque 2021

**« La « nouvelle normalité »
et
les nouveaux enjeux de
cyber-sécurité »**

**Protection du patrimoine informationnel
et sécurité des systèmes d'information**

**Accompagnements de
projets innovants**

**Formation au droit du
numérique et en
protection des
données**

**Conformité
RGPD et audit
protection des
données**

**Dématérialisation
des documents et
des processus**

Ingénierie contractuelle

Commerce électronique

De quoi parle-t-on ?



- « Aspects juridiques du contexte du nouveau modèle de travail ».
- **Nous allons aborder ce sujet sous deux angles :**
 - ✓ L'actualité et les conséquences que la CVOD-19 a pu engendrer en droit des nouvelles technologies/protection des données ;
 - ✓ L'émergence de l'approche Confiance zéro / zéro Confiance / Zero trust et ses conséquences juridiques en matière d'analyse comportementale / l'UEBA.
- Compte tenu du temps imparti, ces sujets seront vus de façon synthétique, en se concentrant sur l'essentiel.



01
—

La COVID 19 quelques impacts juridiques en entreprise

- Dans l'ensemble, l'urgence et la nécessité de s'adapter... aux nouvelles règles et à la situation.
- Le boom des caméras thermiques... puis une interdiction !
 - 7 mai 2020, CNIL : « *interdit aux employeurs [...] de mettre en place des outils de captation automatique de température (telles que des caméras thermiques)* » ;
 - Sachant que les « *prises **manuelles** de température à l'entrée d'un site et sans constitution d'un fichier ni remontée d'information ne sont en revanche pas soumises à la réglementation sur la protection des données personnelles* » ;
 - **Approche diamétralement opposée de l'Autorité de Protection des Données belge.**
- Des contrôles sanitaires qui ont fait irruption dans l'entreprise, via le passe sanitaire et les informations collectées (données de santé, vérifications multiples, etc.).



Télétravail

- Et d'un seul coup le télétravail se généralisa... dans l'urgence !
 - La question de la sécurisation des locaux personnels, des matériels et des connexions ;
 - Le contrôle par la présence remis en cause ;
 - La CNIL et la visioconférence : revenir à l'audio ?
 - L'encadrement des comportements via les chartes... étaient-ils prévus ?





02
—

Le cadre juridique de la « Confiance zéro »

La « Confiance zéro » sous l'angle juridique

- Cf. les analyses de l'ANSSI, les produits proposés par les offreurs, les discussions lors de ce colloque, etc.
- Mais en droit, de quoi parle-t-on ?



Avis scientifique et technique : le modèle Zero Trust de l'ANSSI	RGPD
<ul style="list-style-type: none"> • l'accès basé sur le besoin d'en connaître ; • l'accès donné sur la base du plus faible niveau de privilège nécessaire pour réaliser la tâche ; • les authentifications et autorisations d'accès aux ressources doivent faire l'objet de réévaluations régulières. 	<p>Protection des données par défaut</p>
<ul style="list-style-type: none"> • les demandes d'accès doivent être contrôlées de la même manière quelles que soient leurs origines (le périmètre « intérieur » ou « extérieur » de l'entité) ; • l'entité doit veiller à la sécurité de tous ses actifs à l'occasion des demandes d'accès et de manière récurrente durant l'usage ; 	<p>Protection des données dès la conception</p>
<ul style="list-style-type: none"> • la politique d'accès aux ressources doit être dynamique et prendre en compte un large nombre d'attributs (identités de l'accédant et de la ressource accédée, sensibilité des ressources sollicitées, analyse comportementale de l'utilisateur, horaires d'accès, etc.) ; 	<p>Profilage</p>

Protection des données dès la conception et par défaut

Protection des données dès la conception

- Mesures techniques et organisationnelles
- **Dès l'origine et pendant toute la durée de vie de la donnée**
- But = préserver à tout moment la vie privée et la protection des données

Protection des données par défaut

- Niveau le plus élevé de protection de la vie privée **par défaut**
- Principe de **minimisation**
- Quantité de données, étendue des traitements, durée de conservation, accessibilité, etc.



- Des principes de base en matière de protection des données qui ont été formalisés et inscrits dans le RGPD.
- Peuvent se résumer en :
 - ✓ Sécurisation à toutes les étapes ;
 - ✓ Réduction de la surface d'exposition ;
- **Zéro confiance et RGPD, même combat ?**

Le profilage... qui entraîne un plus grand formalisme

Traitement automatisé

Portant sur des données personnelles

Évaluant des aspects personnels d'un individu notamment pour analyser ou prédire des éléments concernant (...), la fiabilité, le comportement, (...) de cette personne physique

Surveillance de personnes physiques qui sont - en plus - des salariés... donc des « personnes vulnérables » pour la CNIL.

1. Droit du travail : **information/consultation du CSE.**
2. Information **détaillée** des personnels.
3. **Cela a notamment des impacts sur la « charte » interne, dont la rédaction, précise et conforme, est essentielle.**
4. L'incontournable « **Privacy Impact Assessment** » préalable.

Droits renforcées des personnes



- **Droit aux informations « classiques »** requises par le RGPD en matière de traitement de données personnelles ;
- **ET** existence du profilage, logique impliquée, signification et conséquences envisagées d'un tel traitement, fonctionnement du profilage, informations sur les segments / catégories, accès aux données utilisées pour créer le profil et au profil lui-même, etc.
- **Précision renforcée à chaque étape** ... : les inexactitudes peuvent conduire à des prédictions ou des déclarations inappropriées.
- **Le profilage ne doit pas être opaque**: l'information doit être parfaitement claire lorsque le traitement est juridiquement fondé sur le consentement de la personne concernée.
- Droit d'accès au profil lui-même.
- **Droit d'opposition avec test d'équilibrage** prenant en compte l'importance et l'impact, le fardeau de la preuve incombe au contrôleur.

Etude d'Impact sur la Vie Privée (EIVP, AIPD ou PIA) ?

Caractère obligatoire

- Pour les traitements « **susceptibles d'engendrer un risque élevé pour les droits et libertés** ».
 - Le support des neuf critères : **si deux au moins sont réunis, EIVP obligatoire.**
1. Évaluation ou notation (y-compris les activités de profilage ou de prédiction) ;
 2. Surveillance systématique ;
 3. Croisement ou combinaison d'ensembles de données ;
 4. Données concernant des personnes vulnérables.



Contenu

- La description des opérations envisagées, des finalités, voire de l'intérêt légitime poursuivi.
- L'évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités.
- **L'évaluation des risques pour les droits et libertés des personnes concernées** : scénarios décrivant les événements redoutés estimés en termes de gravité et de vraisemblance.
 - La liste des mesures techniques et organisationnelles envisagées pour y faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité (sous-traitants inclus).

Synthèse : vive la confiance zéro !

Informations ? Balance des intérêts ? PIA ? **Rien de bloquant, mais des passages obligés, car...**

- **Sans respect des formalités, les conséquences lors de l'exploitation des preuves face à un salarié :**
 - ✓ **Avant**, des preuves annulées en justice... et un licenciement sans cause réelle et sérieuse ;
 - ✓ **Un retournement de jurisprudence... jusqu'à quand ?** (Cass soc, 25 novembre 2020).
- **De toute façon, le risque des sanctions pour non-conformité au RGPD.**



UP

Avez-vous des questions ?



Merci de votre attention !

UP LEVEL

L E G A L

François COUPEZ

Avocat à la Cour, Associé

14 rue de Tilsitt, 75008 Paris

06 63 12 51 95

fcoupez@level-up.legal



<https://fr.linkedin.com/in/fcoupez/fr>



Certifié Lead Implementer Niveaux
Avancés
ISO / CEI 27001 et ISO / CEI 27701



Droit des nouvelles
technologies / data
(CNB)



Compétences du DPO
Délégué à la protection des données
Agrément CNIL



Certaines images sur cette présentation sont la propriété de la société Adobe (adobe Stock) ou de ses fournisseurs et ayants droits