

Des avocats spécialisés en droit social. Rien d'autre.

— L'expertise de Sotra englobe toutes les branches du droit du travail, de la sécurité sociale et de la fiscalité des travailleurs, dans les secteurs privé et public.

ELLINT Employment & Labor Lawyers International

Trends
LEGAL AWARDS



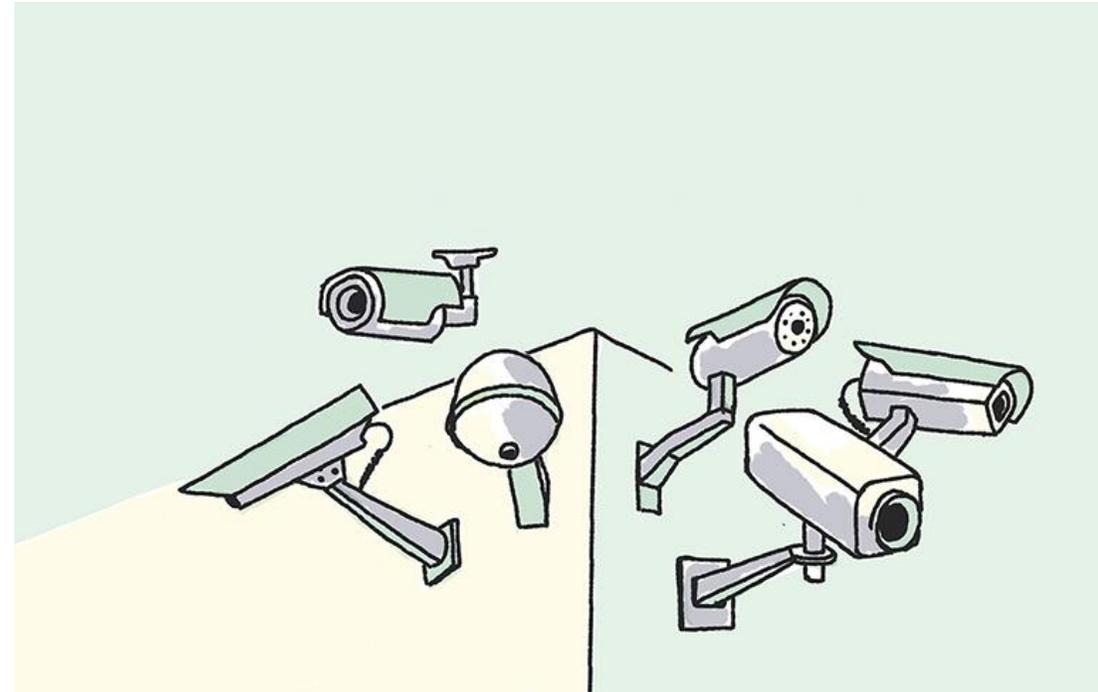
L'utilisation des outils collaboratifs au travail

— Conformité au RGPD et impact sur la relation de travail



Valentin Hanquet
Avocat-associé | Sotra

DPO-Pro
Jeudi 22 septembre 2022



01 Contexte, enjeux & cadre applicable

02 Principes à respecter

03 Quelques cas d'application

01

Contexte, enjeux & cadre applicable



— Contexte & enjeux

- **Contexte**

- 2020-... : nécessité d'organiser le travail à distance/hybride
- Solutions collaboratives nombreuses sur le marché (Urgence >> Conformité légale)
- Pratiques aujourd'hui ancrées, mais méconnaissance/insouciance quant aux caractéristiques techniques et leur utilisation :
 - Sécurité
 - Stockage
 - Partage et transfert de données
 - Etc.

— Contexte & enjeux

- **Enjeux**

- Surveillance potentielle des travailleurs
- Responsabilité de l'employeur/du travailleur en cas de mésusage ?
- + Obligations nouvelles :
 - Consécration du « droit à la déconnexion » des travailleurs : impact ?
 - Protection des lanceurs d'alerte

— Cadre applicable

- **Diversité des textes à combiner**

- Règlement (UE) 2016/679 du 27.04.2016 + loi du 30.07.2018
- C.E.D.H. (art. 8)
- Loi du 13 juin 2005 relative aux communications électroniques (article 124)
- Dispositions pénales :
 - Code pénal (article 314*bis*)
- Réglementation propre aux relations de travail :
 - CCT n°81 du 26 avril 2002
 - Etc.

— Cadre applicable

- CCT n°81 du 26 avril 2002
 - Encadre la protection de la vie privée des travailleurs concernant la surveillance des données relatives aux communications électroniques
 - 2 types de surveillance : (1) les communications électroniques et (2) la surveillance ciblée d'un travailleur

02

Principes à respecter



— Principes

- **Responsabilité**

→ **Traitement potentiel de nombreuses données** par le recours aux outils collaboratifs

→ Obligation de s'assurer, en tant qu'employeur, de la **protection de ces données** :

*« Compte tenu de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement **met en œuvre des mesures techniques et organisationnelles appropriées** pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement. Ces mesures sont réexaminées et actualisées si nécessaire » (art. 24.1 RGPD)*

— Principes

- **Responsabilité**

- Transfert hors UE-EEE : s'assurer que le pays tiers garantit un **niveau de protection équivalent au RGPD**

- Recours à un « **sous-traitant** » :

- Que prévoit le contrat ou l'acte juridique conclu avec le sous-traitant (et ses conditions d'utilisation) ?

- Lui-même soumis au RGPD ?

- Données traitées/transférées ?

- Mesures de protection et sécurité mises en place ?

- Il incombe au RT d'approuver la manière dont les traitements sont effectués

— Principes

- **Responsabilité**

→ Data breach

→ Cas d'application :

- Organisation d'une épreuve en ligne par une université
- Enregistrement vidéo rendu accessible aux utilisateurs de la plateforme et à des tiers
- Mesures immédiates du RT pour retracer et contacter les personnes (26) ayant téléchargé le fichier
- Amende administrative (5.850 EUR) + injonction de notification de la fuite

— Principes

- **Transparence et information**
 - ***Privacy Policy*** intégrant l'utilisation des outils collaboratifs :
 - ✓ Finalités
 - ✓ Enregistrements et utilisation éventuels
 - ✓ Durée de conservation
 - ✓ Etc.

Principes

- Utilisation d'un outil de visioconférence : recommandations de la CNIL

▼ Avant de télécharger une application

> Lors de l'inscription au service

> Lors de l'utilisation

- **Privilégiez les systèmes de visioconférence qui protègent la vie privée.** Vérifiez les conditions d'utilisation de votre logiciel pour vous assurer que ces outils garantissent la confidentialité de vos données et ne les réutilisent pas pour d'autres finalités. L'[ANSSI a certifié Tixeo](#) pour les administrations, les Opérateurs d'Importance Vitale (OIV) et les entreprises soucieuses de leur sécurité. La direction interministérielle du numérique (DINUM) et la Direction Générale de l'Administration et de la Fonction Publique (DGFAP) fournissent un [tableau comparatif](#) pour vous accompagner dans le choix d'une solution qui convient à votre besoin.
- évitez de télécharger l'application depuis un site web ou une source inconnus ;
- n'utilisez que les applications pour lesquelles l'éditeur [vous indique clairement](#) comment vos données sont réutilisées (dans l'application elle-même ou sur son site web, par exemple) ;
- lisez les commentaires des utilisateurs sur des forums de discussion ou, depuis votre téléphone, dans les magasins d'applications ;
- vérifiez que l'éditeur a mis en place des mesures de sécurité essentielles, comme le chiffrement des communications de bout en bout ;
- sécurisez votre réseau Wi-Fi avec un [mot de passe robuste](#), en activant le chiffrement WPA2 ou WPA3 ;
- assurez-vous que votre antivirus et votre pare-feu sont à jour.

Principes

- **Recommandations de la CNIL**

➤ Avant de télécharger une application

▼ Lors de l'inscription au service

➤ Lors de l'utilisation

- lorsque cela est possible, limitez le nombre d'informations fournies lors de l'inscription : utilisez un pseudonyme et une adresse mail dédiée, vérifiez les options de confidentialité proposées lors de la création du compte, etc. ;
- utilisez un **mot de passe** différent de ceux utilisés sur les autres services en ligne ;
- lisez les conditions générales d'utilisation (CGU), notamment ce qui est indiqué en matière de protection des données personnelles, toutes les entreprises fournissant un service à des utilisateurs européens étant tenues d'appliquer le règlement général sur la protection des données (RGPD).

Principes

- recommandations de la CNIL

➤ Avant de télécharger une application

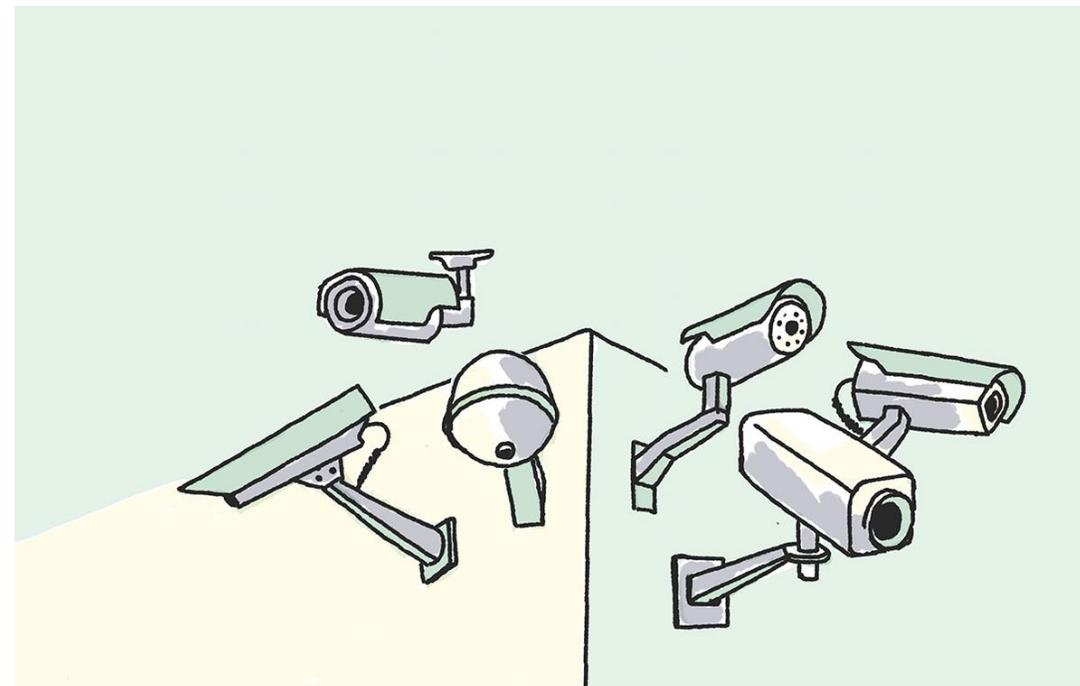
➤ Lors de l'inscription au service

▼ Lors de l'utilisation

- prenez le temps de regarder les paramètres de l'application, notamment en ce qui concerne la protection de votre vie privée (vérifiez, par exemple, s'il existe des options vous permettant de télécharger vos données ou de limiter l'utilisation de certaines informations) ;
- sur votre ordinateur ou votre téléphone, fermez l'application lorsque vous ne l'utilisez plus, notamment si le microphone ou la webcam sont activés ;
- désactivez votre microphone et votre webcam lorsque vous ne les utilisez pas. Vous pouvez également masquer physiquement votre webcam, par exemple avec un bout de ruban adhésif ou un cache ;
- soyez particulièrement vigilant(e) lorsque des personnes mineures utilisent ces services, notamment s'il s'agit de vos élèves.

03

Cas d'application



Le recrutement à distance

- **Contexte**

- Un recruteur recourt à un logiciel de visioconférence pour rencontrer virtuellement les candidats
- Enregistrement des entretiens d'embauche

- **Points d'attention**

- Le recruteur doit s'interroger (et pouvoir justifier) sur le besoin de recourir à cette solution
- Vérifier si les fonctionnalités du logiciel ne permettent pas des traitements incompatibles avec les finalités poursuivies (géolocalisation de l'utilisateur, informations sur le terminal utilisé, accès au carnet d'adresses, etc.)

Le recrutement à distance

- **Finalités**
 - ✓ Simplifier la communication entre les parties
 - ✓ Capturer l'entretien pour une éventuelle utilisation ultérieure
- **Données** : flux audio et vidéo, données de connexion, échange de fichiers ou documents
- **Durée de conservation de l'enregistrement**
 - Sauf justification, pas de conservation au-delà de la décision d'embauche
 - /!\ Enregistrement d'une session paramétré par défaut
 - Durée déterminée selon les besoins effectifs du recruteur
- **Information aux candidats**

La diffusion sur l'intranet de l'entreprise

- **Contexte**

- Visioconférence où la caméra des participants est « ouverte »
- Captures d'écran prises et publiées par la suite sur l'intranet de l'entreprise

- **Points d'attention**

- Les travailleurs bénéficient d'un **droit à l'image**, distinct de la protection de leurs données :

« Ni l'auteur, ni le propriétaire d'un portrait, ni tout autre possesseur ou détenteur d'un portrait n'a le droit de le reproduire ou de le communiquer au public sans l'assentiment de la personne représentée ou celui de ses ayants droit pendant vingt ans à partir de son décès » (art. XI.174 Code de droit économique)

— La diffusion sur l'intranet de l'entreprise

- Nécessité de justifier d'une **base légale** :

« La prise et diffusion de photos ciblées nécessitent une base légale (...).

La Chambre Contentieuse constate que la défenderesse invite ses employés ne souhaitant pas que des photos sur lesquelles ils apparaissent soient enregistrées ni diffusées (...) à contacter le DPR (Data Protection Representative) afin de l'en avertir, et s'engage à ce que ces éventuelles photos soient effacées (...).

Dans cette mesure, la Chambre constate l'absence de violation du droit à l'image du plaignant ».

L'enregistrement caché d'une conversation

- **Les faits**

- Licenciement d'une travailleuse (motif d'insuffisance professionnelle/démotivation)
- Selon la travailleuse, motif inavoué (licenciement-représailles)
- Production en justice de l'enregistrement d'un entretien tenu entre elle et un mandataire de l'employeur
- L'employeur sollicite l'écartement de cet enregistrement, obtenu à son insu

L'enregistrement caché d'une conversation

- **Décision**

- Questions préalables : 1° La preuve est-elle irrégulière ? 2° Par l'affirmative, peut-elle être prise en compte ?
- L'article 8 CEDH ne consacre pas un droit absolu au respect de la vie privée
- En l'espèce, pas de violation de l'article 8 : conversation tenue durant les heures de travail, entre parties, ayant pour objet les conditions d'emploi
- Violation du devoir de loyauté → **Preuve irrégulière**
- Application de la jurisprudence « Antigone » → **Production admissible**

L'enregistrement à des fins d'écolage

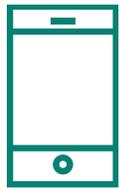
- **Contexte**

- Accès aux enregistrements vidéo des échanges professionnels d'un travailleur (avec fournisseur, client, prospect, etc.)

- **Points d'attention**

- Finalités admissibles : besoin de formation, autre ?
- Information préalable aux personnes concernées
- Activation du dispositif strictement limitée
- Accès réservé aux personnes autorisées
- Autres garanties

Pour nous suivre



SotrApp

L'actualité sociale dans
votre poche



SoCast

Le podcast du droit du
travail belge



SotrAcademy

La première plate-forme de
streaming en droit social belge

Abonnez vous maintenant :

WWW.SOTRACADEMY.BE

Merci pour votre attention !



à Bruxelles

Avenue Louise 65
1050 Bruxelles
+32 (0)2 899 50 50

en Wallonie

Passage de l'Atelier 6 bte 2
5100 Namur (Jambes)
+32 (0)81 39 17 30

WWW.SOTRA.BE