

AURÉLIEN
WITZIG

2026

Professeur à l'Université

Juge à la Cour

Avocat au barreau

Protection des données et surveillance de la communication des travailleurs

2 PLAN



Introduction : les données, la sphère privée et leur protection



Cadre juridique

Loi et jurisprudence suisses
Cour européenne des droits de l'homme



Types de surveillance des communications

Ce qui est admis
Ce qui est interdit
Ce qui est problématique



S'assurer de la licéité de la surveillance : un test en 5 étapes-clefs



Bilan des risques pour l'employeur

3 POURQUOI CE SUJET EST SENSIBLE ?



Généralisation du télétravail, outils numériques, messageries internes



Tensions entre

intérêts légitimes de l'employeur
(sécurité, productivité, conformité)

droits fondamentaux du travailleur
(sphère privée, protection des données)

4 QUESTIONS- CLEFS DE LA CONFÉRENCE



Quelles communications
peuvent être surveillées ?



Sous quelles conditions ?



Quels risques juridiques
concrets pour l'employeur
en Suisse ?

5 LES DONNÉES : DÉFINITIONS (ART. 5 LPD)

Données personnelles

Toutes les informations concernant une personne physique identifiée ou identifiable

Données sensibles

1. les données sur les opinions ou les activités religieuses, philosophiques, politiques ou syndicales,
2. les données sur la santé, la sphère intime ou l'origine raciale ou ethnique,
3. les données génétiques,
4. les données biométriques identifiant une personne physique de manière univoque,
5. les données sur des poursuites ou sanctions pénales et administratives,
6. les données sur des mesures d'aide sociale

6 LE TRAITEMENT DES DONNÉES : RÉGIME JURIDIQUE (ART. 6 LPD)

- **Bonne foi** : respect de la parole donnée, intérêt raisonnable de l'entreprise
- **Finalité** : déterminée, reconnaissable, immuable
- **Proportionnalité** : adéquation du traitement par rapport au but visé, données détruites / anonymisées dès qu'elles ne sont plus nécessaires au regard des finalités du traitement
- **Exactitude**
- **Consentement** en cas de données sensibles
- **Sécurité**

7 CADRE JURIDIQUE

Cadre national

- Constitution fédérale (13)
- Loi sur la protection des données
- Code civil (28) et code des obligations (328b)
- Ordonnance 3 sur le travail (26)

Cadre international

- CEDH (8)
- Balance des intérêts concernant la surveillance des employés (*Barbulescu, Lopez Ribalda, Florindo*)
 - i) Information
 - ii) Degré d'intrusion
 - iii) Motif légitime
 - iv) Caractère intrusif moindre
 - v) Utilisation des résultats de la surveillance
 - vi) Garanties (représentants du personnel, organisme tiers etc.)

8

LA PROTECTION DE LA SPHÈRE PRIVÉE

FAIT PARTIE DE LA PROTECTION DE LA PERSONNALITÉ QUE
L'EMPLOYEUR DOIT GARANTIR (CO 328)

9

CE QUI EST ADMIS

LA SURVEILLANCE DES COMMUNICATIONS PROFESSIONNELLES
EST EN PRINCIPE ADMISE

Communication
professionnelle

= communication
nécessaire à l'exécution
du travail



CE QUI EST INTERDIT

LA SURVEILLANCE DES COMMUNICATIONS **PRIVÉES**
EST EN PRINCIPE INTERDITE

12 MISE EN ŒUVRE : COMMUNICATIONS PROFESSIONNELLES OU PRIVÉES ?

**Principe n° 1 : les
communications
effectuées avec les
outils de l'employeur**

**=
professionnelles**

**Principe n° 2 : les
communications
effectuées durant les
heures de travail**

**=
professionnelles**

**Principe n° 3 : les
communications
effectuées avec les
outils du travailleur**

= privées

**Principe n° 4 : les
communications
effectuées hors des
heures de travail**

= privées

I3 TEMPÉRAMENTS

- Les travailleurs peuvent désigner comme **privées** certaines communications.
- Les communications dont il est clairement reconnaissable qu'elles ne sont pas professionnelles doivent être considérées comme **privées**.
- Les communications **professionnelles** même effectuées avec les outils personnels du travailleur et / ou hors du temps de travail officiel doivent pouvoir être contrôlées par l'employeur.

I 4 LA SURVEILLANCE DES COMMUNICATIONS : CE QUI EST PROBLÉMATIQUE

01

Comment procéder pour distinguer si une communication est professionnelle ou privée ?

02

Comment contrôler que le travailleur respecte les consignes sur l'usage professionnel des outils et du temps de travail ?

I5 DISTINGUER SI UNE COMMUNICATION EST PROFESSIONNELLE OU PRIVÉE

Contrat de travail / règlement d'entreprise

=> prévoir une règle de distinction privé/pro

Observer les classifications du travailleur

=> dossier «Privé», «Personnel»

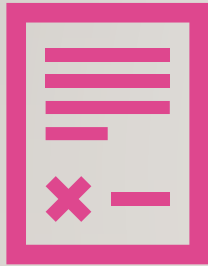
Observer le destinataire de la communication

=> client de l'entreprise ? ami ? famille ?

Analyser le contenu

=> s'arrêter si clairement privé

16 CONTRÔLER SI LE TRAVAILLEUR RESPECTE LES CONSIGNES



Mettre en place une réglementation contractuelle / d'entreprise



Procéder à des contrôles

Non ciblés

Non permanents

Non comportementaux

LES CONTRÔLES : PROCESSUS

Recommandations (à adapter suivant les circonstances)

- Contrôle annoncé / prévu à intervalles réguliers
- Contrôle en présence du travailleur / d'un représentant du personnel / d'un RH «neutre» / d'un tiers professionnel de confiance
- Contrôle non annoncé consécutif à des risques professionnels manifestes / des abus manifestes

18 SI L'EMPLOYEUR A INTERDIT L'USAGE PRIVÉ DES OUTILS DE COMMUNICATION MIS À DISPOSITION

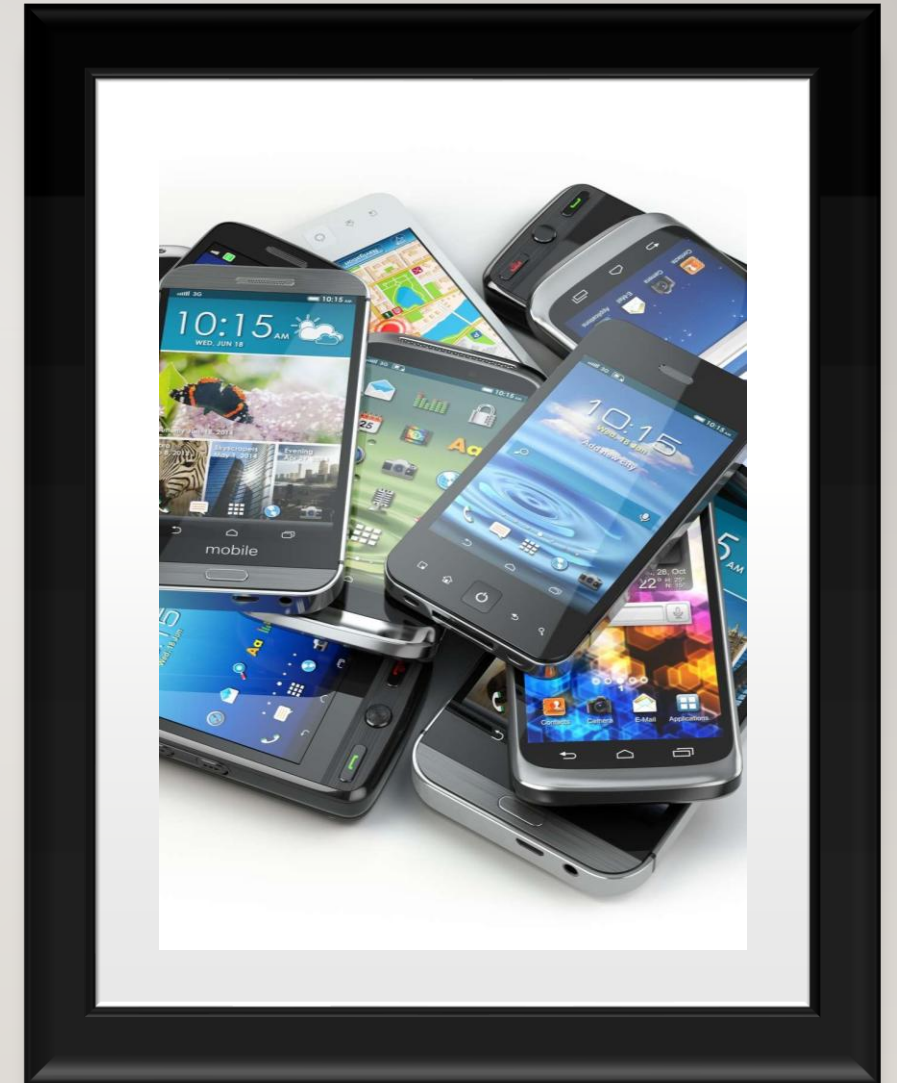
L'employeur peut contrôler plus largement que les communications du travailleur sont uniquement professionnelles.



L'employeur n'est pas pour autant autorisé à lire / écouter les communications privées => constater l'usage interdit suffit.

19 AFFAIRE DU GROUPE WHATSAPP (TF, 25 AOÛT 2021, 4A_518/2020)

- L'employeuse récupère les messages échangés (puis effacés) dans un groupe whatsapp par un employé => Elle considère que ces éléments prouvent qu'il ne fait pas les heures supplémentaires annoncées et qu'il n'est pas capable de gérer ses équipes.
- En réalité, l'employeuse cherchait des preuves pour accabler son employé.
- Si elle voulait protéger d'autres salariés, l'employeuse pouvait utiliser des procédés moins incisifs (p. ex. interroger les autres collaborateurs ou des témoins).
- L'employeuse «jette en pâture» la vie privée de son salarié pour des intérêts purement financiers.





Si possible : attendre son retour



Si attente impossible : ouvrir l'ordinateur /
le téléphone en présence d'un représentant
du personnel / d'un RH de confiance / d'un
tiers professionnel



Ne lire / écouter que ce qui est
professionnel

CAS PRATIQUE N° I : 20 COLLABORATEUR ABSENT

21 CAS PRATIQUE N° 2 : LE SOUPÇON D'ABUS



Procéder régulièrement à des contrôles anonymes non ciblés

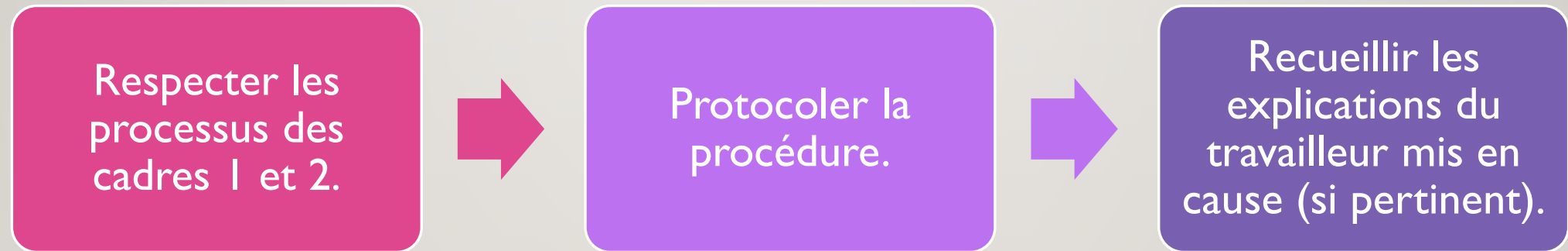


Ne procéder à des investigations plus poussées que si l'abus / le risque pour l'entreprise est identifié



Prévenir la personne (si pertinent) puis procéder comme au cas n° 1

22 CAS PRATIQUE N° 3 : L'ENQUÊTE INTERNE (*HARCÈLEMENT, FRAUDE, ETC.*)



23 S'ASSURER DE LA LICÉITÉ DE LA SURVEILLANCE DES COMMUNICATIONS : UN TEST EN 5 ÉTAPES-CLEFS



Respecter le cadre mis en place : Contrat ? Règlement ? Loi ?



N'agir qu'en cas de preuves ou de soupçons graves et confirmés



Procéder à l'observation des communications en présence de personnes pertinentes : Le travailleur ? Un représentant du personnel ? Un professionnel neutre ? Un tiers de confiance ?



N'utiliser le résultat de l'observation que de manière proportionnée et justifiée par l'intérêt objectif de l'entreprise.



Détruire toute donnée récoltée une fois que son traitement n'est plus justifié.

24 BILAN DES RISQUES POTENTIELS POUR L'EMPLOYEUR

Action en protection de la personnalité du travailleur (CC 28a, LPD 32)

- Interdiction d'utiliser les communications personnelles
- Destruction des communications personnelles
- Réparation du tort moral

Inexploitation en procédure de la preuve obtenue illicitement

- La preuve peut quand même être prise en considération si intérêt prépondérant à la manifestation de la vérité (CPC I 52)

+ Risque pénal



25 À RETENIR

La surveillance n'est **pas interdite**, mais **encadrée**.

La **préparation en amont** (règlementation, information, choix avant d'agir) est déterminante.

Le risque juridique se joue souvent sur les **mise en œuvre opérationnelle**.



26

QUESTIONS

