



PRESTO N°135 / Janvier 2026

L'impact du
déploiement

RPPS+

et de la **E-CPS**

sur les conditions de travail
dans l'action sociale

PRESTO N°135 / Janvier 2026

L'impact du
déploiement

RPPS+

et de la **E-CPS**

sur les conditions de travail
dans l'action sociale

N°135

PRESTO

SOMMAIRE

L'IMPACT DU DÉPLOIEMENT RPPS+ ET DE LA E-CPS SUR LES CONDITIONS DE TRAVAIL DANS L'ACTION SOCIALE.....	3
CHAPITRE I : L'ARCHITECTURE DU RPPS+ ET LA FIN PROGRAMMÉE DE LA CARTE PHYSIQUE.....	4
1.1. La bascule historique : De ADELI au RPPS	4
1.2. Le mécanisme d'enregistrement : Le portail RPPS+	4
1.3. La stratégie du « Mobile First » et l'exclusion de la carte physique.....	5
CHAPITRE II : LE CADRE JURIDIQUE DE L'OBLIGATION DE MOYENS	6
2.1. Le principe fondamental : L'employeur fournit l'outil	6
2.2. L'Accord National Interprofessionnel (ANI) et le télétravail	6
2.3. L'intégrité de la vie privée (Article L. 1121-1).....	7
2.4. La question de la "force majeure" numérique	7
CHAPITRE III : BYOD ET RGPD - LES RISQUES POUR LA SÉCURITÉ DES DONNÉES ...	8
3.1. L'employeur : responsable de traitement.....	8
3.2. La "conteneurisation" et l'intrusion technique	8
3.3. Risque de saisie judiciaire.....	9
CHAPITRE IV : SANTÉ AU TRAVAIL ET DROIT À LA DÉCONNEXION	10
4.1. L'hyperconnexion et les Risques Psychosociaux (RPS).....	10
4.2. La sécurité des travailleurs isolés (PTI/DATI).....	10
CHAPITRE V : ANALYSE SECTORIELLE (CCN 66, CCN 51) ET FINANCEMENT	12
5.1. Convention Collective du 15 mars 1966 (CCN 66)	12
5.2. Convention Collective du 31 octobre 1951 (CCN 51 - FEHAP)	12
5.3. Le mythe du "manque de budget" et le Ségur du numérique.....	12
CHAPITRE VI : TABLEAU COMPARATIF DES OPTIONS ET COÛTS.....	14
CHAPITRE VII : STRATÉGIE SYNDICALE ET MODÈLES D'ACTION.....	16
7.1. Phase 1 : Prévention et information	16
7.2. Phase 2 : interpellation en CSE.....	16
7.3. Phase 3 : Négociation d'un accord (Si le BYOD est inévitable)	16
7.4. Phase 4 : Le refus individuel et collectif.....	17
CONCLUSION	18

L'IMPACT DU DÉPLOIEMENT RPPS+ ET DE LA E-CPS SUR LES CONDITIONS DE TRAVAIL DANS L'ACTION SOCIALE

Le secteur social et médico-social connaît actuellement une mutation numérique sans précédent, orchestrée par les pouvoirs publics dans le cadre du Ségur du Numérique en Santé. Cette transformation, matérialisée par l'extension du Répertoire Partagé des Professionnels de Santé (RPPS) aux acteurs du social via le portail RPPS+, vise à fluidifier le partage des données usagers et à sécuriser les parcours de soin et d'accompagnement. Si la Fédération Nationale de l'Action Sociale FO (FNAS-FO) ne s'oppose pas par principe à la modernisation des outils, elle alerte vigoureusement sur les modalités de sa mise en œuvre technique et matérielle.

Le cœur du conflit réside dans le dispositif d'authentification forte retenu par l'Agence du Numérique en Santé (ANS) : la « e-CPS ». Contrairement à la carte CPS physique traditionnelle, la e-CPS est une application mobile nécessitant un smartphone. Or, une large part des employeurs du secteur associatif et public refusent d'investir dans une flotte de terminaux professionnels, exerçant une pression tacite ou explicite pour que les salariés installent cette application professionnelle sur leurs terminaux personnels (BYOD - *Bring Your Own Device*).

Ce Presto a pour objet de fournir aux adhérents, délégués syndicaux et élus CSE de la FNAS-FO un arsenal juridique complet pour contester cette dérive. Il démontre, à l'appui du Code du travail, de la jurisprudence de la Cour de cassation et des délibérations de la CNIL, que l'imposition du téléphone personnel constitue un transfert de charges illégal, une atteinte disproportionnée à la vie privée et un risque majeur pour la sécurité des données.

Ce Presto est structuré pour servir de base de négociation et de contestation. Elle détaille l'architecture technique du RPPS+ pour mieux en déconstruire les contraintes, analyse les obligations de l'employeur en matière de fourniture de matériel, et propose une stratégie syndicale offensive pour exiger l'équipement professionnel ou, à défaut, une indemnisation juste et encadrée.

CHAPITRE I : L'ARCHITECTURE DU RPPS+ ET LA FIN PROGRAMMÉE DE LA CARTE PHYSIQUE

Pour comprendre la coercition qui s'exerce sur les salariés concernant l'usage de leur smartphone personnel, il est impératif de disséquer l'écosystème technique imposé par l'État. Ce n'est pas une simple "mise à jour logicielle", mais un changement de paradigme dans l'identification du travailleur social.

1.1. La bascule historique : De ADELI au RPPS

Jusqu'à récemment, l'identification des professionnels du secteur social et médico-social reposait sur des systèmes disparates ou le répertoire ADELI, qui s'avérait obsolète et peu interopérable. Le Ségur du Numérique en Santé a acté la bascule de l'ensemble des professionnels intervenant dans le parcours de soin et d'accompagnement vers le Répertoire Partagé des Professionnels de Santé (RPPS), historiquement réservé aux médecins, pharmaciens et sages femmes.

Cette extension concerne désormais les professions dites « à rôle », c'est-à-dire les professionnels qui n'ont pas d'ordre professionnel mais qui jouent un rôle crucial dans la prise en charge : éducateurs spécialisés, assistants de service social, accompagnants éducatifs et sociaux (AES), aides médico-psychologiques (AMP), moniteurs éducateurs, et directeurs d'établissements. L'objectif est de leur attribuer un identifiant unique et pérenne (le numéro RPPS à 11 chiffres) qui les suivra tout au long de leur carrière, quel que soit leur employeur.

1.2. Le mécanisme d'enregistrement : Le portail RPPS+

Contrairement aux médecins qui s'enregistrent auprès de leur Ordre, les professionnels du social doivent être enregistrés par leur employeur via le portail RPPS+. Cette procédure place la structure employeuse au centre du dispositif de validation de l'identité numérique.

1.2.1. Le rôle pivot de l'employeur (gestionnaire)

Le gestionnaire RPPS+ est la personne désignée par la structure (souvent la direction ou les RH) pour administrer les comptes des salariés. Ce gestionnaire accède au portail via sa propre authentification forte (carte CPS de directeur ou certificat de structure). C'est lui qui atteste de la fonction du salarié et active son identité numérique. Cela crée une dépendance administrative : le droit d'accès aux outils numériques du salarié (Dossier Usager Informatisé - DUI, Messagerie Sécurisée de Santé) est conditionné par cet enregistrement patronal.

1.2.2. La collecte des données personnelles

Lors de l'enregistrement sur le portail RPPS+, l'employeur doit renseigner les données d'état civil du salarié mais également des données de contact. C'est ici que le piège matériel se referme : le formulaire demande un numéro de téléphone mobile et une adresse email. L'Agence du Numérique en Santé (ANS) précise : « Faut-il nécessairement renseigner un numéro de téléphone lors de l'enregistrement? Oui, ce numéro sera nécessaire pour que le professionnel utilise sa e-CPS via l'application sur smartphone ».

Si l'employeur ne fournit pas de téléphone professionnel, il est contraint de demander – et souvent d'exiger – le numéro personnel du salarié pour finaliser l'inscription technique, initiant de fait le mélange des genres entre vie privée et vie professionnelle.

1.3. La stratégie du « Mobile First » et l'exclusion de la carte physique

L'enjeu central pour la FNAS-FO est la disparition progressive du support physique d'authentification pour les non-médicaux.

1.3.1. La hiérarchie des moyens d'authentification

Pour accéder aux services via le protocole « Pro Santé Connect » (l'équivalent de France Connect pour la santé), deux moyens existent :

1. **La Carte CPS (Carte de Professionnel de Santé)** : C'est une carte à puce physique (smartcard) nécessitant un lecteur USB connecté à un ordinateur. Elle est gratuite, sécurisée, et garantit le droit à la déconnexion (une fois la carte retirée, on n'est plus connecté). Cependant, l'ANS et les ARS restreignent sa distribution. Elle est prioritairement réservée aux professions à ordre (médecins, infirmiers) et aux représentants légaux des structures.
2. **La e-CPS (application mobile)** : C'est le moyen privilégié et poussé par l'administration pour la masse des salariés du secteur social. C'est une application à installer sur un smartphone (Android ou iOS) qui sert de clé d'authentification.

1.3.2. L'absence de carte physique pour le secteur social

Les documents techniques sont sans ambiguïté : « A ce jour, il n'est pas prévu qu'il y ait de carte physique pour les professionnels enregistrés via le RPPS+ ». Cette phrase est capitale. Elle signifie que par défaut, l'État a conçu le système pour fonctionner sur smartphone, sans prévoir le budget ou la logistique pour équiper des centaines de milliers d'éducateurs et d'aides à domicile en cartes à puce et lecteurs.

Cette carence structurelle de l'État et des éditeurs logiciels crée un report de charge vers l'employeur, qui le reporte à son tour sur le salarié. Le salarié se retrouve être la variable d'ajustement budgétaire d'une dématérialisation mal financée.

1.3.3. Les contraintes techniques de la e-CPS

L'application e-CPS n'est pas anodine. Elle exige :

- **Un OS récent** : Android 6+ ou iOS récent. Les salariés ayant des téléphones anciens sont exclus ou contraints de changer d'appareil à leurs frais.
- **Un verrouillage écran** : L'application impose souvent que le téléphone soit sécurisé par code ou biométrie, modifiant les habitudes d'usage du propriétaire.
- **Une connexion Internet** : L'usage de la data personnelle est requis pour valider l'authentification à chaque connexion.
- **Des permissions intrusives** : Accès à la caméra (pour scanner les QR codes de connexion), aux notifications, et à l'état du téléphone.

CHAPITRE II : LE CADRE JURIDIQUE DE L'OBLIGATION DE MOYENS

Face à la pression managériale invoquant la modernisation ou la simplicité, le délégué syndical doit revenir aux fondamentaux du droit du travail : le lien de subordination implique la fourniture des moyens.

2.1. Le principe fondamental : L'employeur fournit l'outil

Le contrat de travail se définit par la fourniture d'une prestation de travail contre rémunération, dans un lien de subordination. Il n'appartient pas au salarié de subventionner son employeur en fournissant son propre outil de production.

2.1.1. Jurisprudence constante de la chambre sociale

La Cour de cassation a établi une jurisprudence extrêmement ferme sur les frais professionnels. Dans son arrêt de principe du 25 février 1998 (et réaffirmé constamment, notamment Cass. Soc. 12 décembre 2012, n° 11-26.585), la Cour énonce que : « Les frais qu'un salarié justifie avoir exposés pour les besoins de son activité professionnelle et dans l'intérêt de l'employeur doivent lui être remboursés sans qu'ils ne puissent être imputés sur sa rémunération ».

Cette règle est d'ordre public. Aucune clause du contrat de travail ne peut y déroger défavorablement. Si l'accès au DUI (Dossier Usager Informatisé) est nécessaire pour travailler, le terminal permettant cet accès est un frais professionnel.

2.1.2. L'interdiction des sanctions pécuniaires

L'article L. 1331-2 du Code du travail interdit les sanctions pécuniaires. Or, obliger un salarié à utiliser son forfait personnel et à user la batterie de son téléphone personnel pour le travail revient à diminuer son salaire net du montant de ces coûts. C'est une sanction pécuniaire déguisée et illégale.

2.2. L'Accord National Interprofessionnel (ANI) et le télétravail

Bien que le sujet dépasse le strict cadre du télétravail (concerne aussi les visites à domicile ou le travail sur site sans PC fixe), les textes sur le télétravail servent de référence juridique pour l'équipement numérique.

L'Accord National Interprofessionnel du 26 novembre 2020, étendu par arrêté, et l'accord du 7 juillet 2022 sont explicites. L'article 8 de l'accord de 2022 précise : « L'employeur sera tenu de fournir un téléphone portable ou à défaut, un système de communication numérique ».

Cette obligation s'étend par analogie à toute situation de mobilité ou de dématérialisation imposée. L'employeur ne peut arguer que le salarié possède déjà un téléphone pour s'exonérer de cette obligation. La propriété privée du salarié n'est pas un actif de l'entreprise.

2.3. L'intégrité de la vie privée (Article L. 1121-1)

L'article L. 1121-1 du Code du travail est la pierre angulaire de la défense des libertés individuelles en entreprise : « Nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché ».

2.3.1. Disproportion de la mesure BYOD

Imposer l'installation d'une application professionnelle sur un smartphone personnel est-il proportionné ?

- **Non**, car des alternatives existent (fourniture d'un téléphone pro, fourniture d'une carte physique via un lecteur sur PC partagé, ou clé OTP physique).
- **Non**, car l'intrusion est permanente (notifications, présence de l'icône "boulot" à côté des photos de famille).
- **Non**, car cela expose le salarié à des risques juridiques (voir Chapitre IV sur les données).

2.3.2. Le droit de refus légitime

Un salarié peut refuser d'installer la e-CPS sur son téléphone personnel. Ce refus ne peut constituer une faute et ne peut justifier une sanction disciplinaire.

Toute sanction (avertissement, mise à pied) fondée sur ce refus serait nulle de plein droit. L'employeur qui sanctionnerait un salarié pour ce motif commettrait un abus de pouvoir, car il sanctionnerait le salarié pour le refus de pallier la carence matérielle de l'entreprise.

2.4. La question de la "force majeure" numérique

Les employeurs arguent souvent qu'ils sont obligés par l'État et l'ANS de passer à la e-CPS et qu'ils n'ont pas le choix. Juridiquement, cet argument est inopérant vis-à-vis du salarié. L'obligation administrative de l'employeur envers l'ARS ou l'ANS ne transfère pas l'obligation de moyens sur le salarié. C'est à l'entreprise de se mettre en conformité avec les exigences de l'État, en investissant les sommes nécessaires. La contrainte technique externe ne suspend pas le droit du travail.

CHAPITRE III : BYOD ET RGPD - LES RISQUES POUR LA SÉCURITÉ DES DONNÉES

Le BYOD (*Bring Your Own Device*), ou AVEC (*Apportez Votre Équipement Personnel*), est souvent présenté comme une facilité. C'est en réalité un cauchemar juridique en matière de protection des données (RGPD), que la CNIL (Commission Nationale de l'Informatique et des Libertés) encadre très strictement.

3.1. L'employeur : responsable de traitement

Selon le Règlement Général sur la Protection des Données (RGPD), l'employeur est le responsable de traitement des données usagers manipulées par ses salariés. Il a une obligation de sécurité (Article 32 du RGPD).

3.1.1. La perte de contrôle sur le terminal

En autorisant ou en obligeant l'usage de smartphones personnels, l'employeur perd la maîtrise de la sécurité du terminal :

- Il ne peut garantir que le téléphone est à jour (correctifs de sécurité Android/iOS).
- Il ne peut garantir l'absence de logiciels malveillants installés par le salarié ou sa famille (jeux, apps tierces).
- Il ne peut imposer un mot de passe complexe sans empiéter sur la vie privée.
- Il ne peut chiffrer le stockage du téléphone à distance.

3.1.2. La responsabilité en cas de violation de données

Si un salarié perd son téléphone personnel contenant des données professionnelles (ou donnant accès à celles-ci via la e-CPS et le webmail resté ouvert), c'est l'employeur qui est responsable devant la CNIL. Il doit notifier la violation sous 72 heures.

L'argument syndical est ici de retourner la responsabilité vers la direction : « Monsieur le Directeur, en refusant d'acheter des téléphones sécurisés, vous engagez votre responsabilité pénale et celle de la structure en cas de fuite de données d'usagers vulnérables. La FNAS-FO vous met en garde officiellement contre ce risque. »

3.2. La "conteneurisation" et l'intrusion technique

Pour sécuriser le BYOD, la CNIL recommande des solutions de "conteneurisation" ou MDM (*Mobile Device Management*) qui créent une bulle étanche professionnelle sur le téléphone personnel.

3.2.1. Les limites du MDM sur téléphone perso

L'installation d'un MDM sur un appareil privé est techniquement possible mais juridiquement explosive :

- **Effacement à distance** : En cas de perte ou de départ du salarié, l'employeur peut envoyer une commande d'effacement ("remote wipe"). Sur un téléphone mal configuré,

cela peut effacer *tout* le téléphone, y compris les photos de vacances et les contacts personnels.

- **Surveillance** : Les agents MDM peuvent théoriquement remonter des infos sur les applications installées, la localisation (si GPS actif), ou l'état du réseau. Même si l'employeur jure ne pas regarder, la possibilité technique existe, créant un climat de suspicion.

3.2.2. L'avis de la CNIL

La CNIL reste très réservée sur le BYOD et privilégie toujours la fourniture de terminaux dédiés. Elle précise : « Des mesures spécifiques doivent être prises pour protéger les informations personnelles en les isolant des informations professionnelles ». Or, ces mesures sont coûteuses. Paradoxalement, bien sécuriser un BYOD coûte parfois aussi cher en licences logicielles que d'acheter un téléphone d'entrée de gamme.

3.3. Risque de saisie judiciaire

C'est un point souvent ignoré mais critique dans le secteur social.

En cas d'enquête judiciaire (maltraitance supposée, accident grave d'un usager, plainte d'une famille), les outils de travail peuvent être saisis par la police ou la justice pour expertise.

- **Si le téléphone est professionnel** : Seul le téléphone pro est saisi. Le salarié garde son téléphone perso et sa vie privée.
- **Si le téléphone est personnel (BYOD)** : La justice saisit le téléphone personnel du salarié. Il est placé sous scellés pour une durée indéterminée (mois ou années). Le salarié perd l'accès à sa vie numérique privée, ses photos, ses contacts, ses applications bancaires.

L'employeur ne pourra pas empêcher cette saisie. C'est un risque inacceptable pour le salarié.

CHAPITRE IV : SANTÉ AU TRAVAIL ET DROIT À LA DÉCONNEXION

L'impact du smartphone personnel dépasse le cadre juridique technique ; il touche à la santé mentale et à la définition même du temps de travail.

4.1. L'hyperconnexion et les Risques Psychosociaux (RPS)

La FNAS-FO a fait de la lutte contre les RPS une priorité. Le mélange des genres induit par le RPPS+ sur smartphone personnel est un facteur aggravant.

4.1.1. La charge mentale de la notification

Avoir ses outils professionnels dans sa poche 24h/24 crée une disponibilité cognitive permanente. Même si le salarié ne répond pas, voir une notification d'email ou d'alerte métier le samedi soir déclenche un stress.

Cette porosité est contraire à l'obligation de sécurité de résultat de l'employeur en matière de protection de la santé (Article L. 4121-1).

4.1.2. Le droit à la déconnexion (Loi El Khomri)

Depuis 2017, le droit à la déconnexion est inscrit dans le Code du travail (Art. L. 2242-17). Il doit faire l'objet d'une négociation annuelle (NAO).

Sur un téléphone professionnel, la déconnexion est simple : on éteint l'appareil ou on le laisse au bureau.

Sur un téléphone personnel, la déconnexion est complexe : elle demande une manipulation active (aller dans les paramètres, couper les notifs de l'appli spécifique). Cette charge de la déconnexion ne doit pas reposer sur la volonté du salarié.

Revendication FO : Si le BYOD est toléré (par accord), l'application professionnelle doit disposer d'une fonctionnalité de blocage horaire automatique, empêchant toute notification hors des plages de travail.

4.2. La sécurité des travailleurs isolés (PTI/DATI)

Dans l'action sociale (SAD, SAVS, SAMSAH), de nombreux salariés interviennent seuls au domicile ou en extérieur. La protection du travailleur isolé (PTI) ou Dispositif d'Alarme pour Travailleur Isolé (DATI) est une obligation légale.

4.2.1. L'inadéquation du smartphone personnel

Les employeurs tentent parfois d'installer des applis PTI sur les téléphones perso. C'est dangereux :

- En cas de batterie vide (usure perso), l'alarme ne part pas.
- En cas de zone blanche ou de forfait data épuisé, l'alarme ne part pas.
- La géolocalisation permanente requise pour le PTI est une intrusion majeure sur un téléphone privé.

Pour FO, la sécurité ne se négocie pas. Les travailleurs isolés doivent être équipés de terminaux professionnels dédiés, robustes, avec bouton SOS physique et réseau prioritaire ou multi-opérateurs, ce qu'un smartphone grand public ne garantit pas.

CHAPITRE V : ANALYSE SECTORIELLE (CCN 66, CCN 51) ET FINANCEMENT

Les conventions collectives nationales offrent des leviers spécifiques, et la question du financement doit être démystifiée.

5.1. Convention Collective du 15 mars 1966 (CCN 66)

La CCN 66, majoritaire dans le secteur du handicap, ne contient pas de dispositions explicites sur le BYOD (elle date d'une époque pré-numérique). Cependant :

- **Classification et Outils** : Les fiches métiers et la définition des postes impliquent que l'employeur fournit le cadre de travail.
- **Frais de déplacement et mission** : L'article 11 et l'annexe sur les frais de déplacement sont stricts sur le remboursement. Par analogie, tout frais engagé pour la mission doit être remboursé.
- **Stratégie FO** : Utiliser les NAO pour inclure une clause "Matériel" dans les accords d'entreprise, en s'appuyant sur l'absence de clause contraire dans la CCN.

5.2. Convention Collective du 31 octobre 1951 (CCN 51 - FEHAP)

La CCN 51 est plus précise sur les conditions d'exécution.

- **Article 02.04 (Hygiène et Sécurité)** : L'employeur doit veiller à la sécurité. L'argument PTI/DATI est très fort ici.
- **Avenants Numériques** : La branche sanitaire et sociale associative (BASS) discute d'avenants sur le numérique. FO y défend le principe « 1 salarié = 1 outil fourni ». Il faut surveiller les accords de branche récents qui pourraient encadrer le télétravail et l'équipement.

5.3. Le mythe du "manque de budget" et le Ségur du numérique

L'argument budgétaire est le bouclier favori des directions. Il est souvent fallacieux dans le contexte actuel.

5.3.1. Le programme SONS (Système Ouvert et Non Sélectif)

Le Ségur du Numérique a débloqué 600 millions d'euros pour le médico-social sur la période 2021-2025. Ce financement vise l'acquisition de logiciels (DUI) compatibles, mais aussi la mise à niveau des infrastructures.

- Les financements « ESMS Numérique » pilotés par les ARS (Agences Régionales de Santé) incluent des volets d'équipement matériel (tablettes, PC, smartphones) pour favoriser la mobilité.
- L'employeur perçoit des aides à l'usage pour l'atteinte de cibles d'utilisation du DMP et de la MSSanté.

5.3.2. L'argumentaire FO

L'argent public est là. Les dotations Ségur ne doivent pas servir uniquement à payer des licences logicielles onéreuses à des éditeurs privés, mais aussi à équiper les salariés qui produisent la donnée.

Il faut exiger en CSE la transparence sur l'utilisation des fonds « Ségur Numérique » et « ESMS Numérique ». Si l'employeur a touché une subvention pour la transformation numérique, une partie doit être fléchée vers l'achat de terminaux.

CHAPITRE VI : TABLEAU COMPARATIF DES OPTIONS ET COÛTS

Pour objectiver le débat en négociation, nous comparons les trois scénarios possibles.

Critère	Option 1 : Flotte mobile professionnelle (Revendication FO)	Option 2 : BYOD (Téléphone perso) (scénario "sauvage" ou négocié)	Option 3 : Carte CPS physique + PC partagé (solution de repli)
Coût pour le salarié	0 €	Abonnement data + Amortissement mobile + Usure batterie + Accessoires	0 €
Vie privée / RGPD	Protection maximale (Séparation physique)	Intrusion forte (Mélange des données, géolocalisation possible, risque saisie)	Protection maximale
Droit à la déconnexion	Garanti (Téléphone éteint ou laissé au bureau)	Menacé (Nécessite discipline et paramétrage complexe)	Garanti (Carte retirée = déconnexion)
Sécurité des données	Maîtrise totale par l'employeur (MDM, chiffrement)	Risque critique (Vol, malware, OS obsolète)	Haute (Cryptographie matérielle)
Responsabilité (Casse/Vol)	Employeur (sauf faute lourde)	Salarié (sauf clause contraire spécifique)	Salarié (pour la carte uniquement)

Compatibilité RPPS+	100 %	100 %	Faible (L'ANS ne délivre pas de cartes à tous les métiers sociaux)
Coût pour l'employeur	Élevé (Achat + abo + gestion) mais amortissable et TVA récupérable	Nul (si sauvage) ou faible (si indemnité)	Faible (Achat lecteurs de cartes)
Position FNAS-FO	À EXIGER	À REFUSER (sauf accord blindé avec forte indemnité)	À ACCEPTER pour les postes sédentaires

Tableau 1 : Comparatif des modalités d'accès au RPPS+ et impacts salariés

CHAPITRE VII : STRATÉGIE SYNDICALE ET MODÈLES D'ACTION

Face à l'offensive patronale sur le BYOD, la FNAS-FO propose une stratégie graduée : Information, interpellation, négociation ou refus.

7.1. Phase 1 : Prévention et information

Ne pas attendre que la direction impose l'application « e-CPS ».

- **Tractage** : Informer les salariés que l'installation n'est pas obligatoire sur leur matériel perso.
- **Enquête Flash** : Recenser qui utilise déjà son téléphone perso. Ces données chiffrées ("80% de l'équipe utilise son forfait perso") sont une arme en CSE pour démontrer le travail dissimulé (non-paiement de frais).

7.2. Phase 2 : interpellation en CSE

Le CSE doit être consulté *avant* tout projet d'introduction de nouvelles technologies (Art. L. 2312-8). Le passage au RPPS+ et l'usage de la e-CPS constituent une modification importante des conditions de travail.

- **Motion à déposer** : "Le CSE demande la suspension du déploiement de la e-CPS sur terminaux personnels tant qu'une étude d'impact RGPD et RPS n'a pas été présentée, et qu'une solution matérielle fournie par l'employeur n'est pas garantie."
- **Expertise** : Si le projet est vaste, le CSE peut voter une expertise "Conditions de travail et Politique Sociale" financée par l'employeur pour évaluer les risques du BYOD.

7.3. Phase 3 : Négociation d'un accord (Si le BYOD est inévitable)

Si le rapport de force ne permet pas d'obtenir 100% de téléphones pros, il faut négocier un accord d'entreprise encadrant le BYOD. Cet accord doit impérativement contenir :

1. **Le principe du volontariat écrit** : Avenant au contrat de travail, révoquant le salarié à tout moment (avec délai de prévenance).
2. **L'indemnité forfaitaire mensuelle** : FO revendique un montant couvrant l'abonnement pro et l'usure. Base de négociation : **20€ à 30€ net / mois**. (L'URSSAF admet des forfaits, il faut viser le haut de la fourchette pour dissuader l'employeur).
3. **La fourniture d'accessoires** : Coque de protection, batterie externe, chargeur fournis par l'employeur.
4. **La clause de non-responsabilité** : Le salarié ne peut être tenu responsable du vol, de la casse ou du piratage de son téléphone perso dans le cadre professionnel.
5. **Le protocole de fin de contrat** : Comment les données pro sont-elles effacées sans toucher aux données perso ?

7.4. Phase 4 : Le refus individuel et collectif

Si l'employeur passe en force sans indemnité, le refus est la seule option.

Modèle de lettre de refus (À personnaliser)

Objet : Refus d'utilisation de mon matériel téléphonique personnel et demande de mise à disposition de matériel professionnel

Monsieur le Directeur / Madame la Directrice,

Vous m'avez sollicité(e) pour procéder à l'enregistrement de mon identité numérique sur le portail RPPS+ et pour installer l'application « e-CPS » sur mon smartphone personnel.

Je tiens à vous informer que je ne dispose pas d'un équipement téléphonique professionnel fourni par l'association/l'établissement.

Conformément à la jurisprudence constante de la Cour de cassation (notamment Soc. 25 février 1998 et 12 décembre 2012) et aux dispositions de l'Accord National Interprofessionnel sur le télétravail et la numérisation, il appartient à l'employeur de fournir les moyens nécessaires à l'accomplissement de la prestation de travail.

L'utilisation de mon terminal personnel (achat, maintenance) et de mon abonnement téléphonique privé à des fins professionnelles constitue une immixtion injustifiée dans ma vie privée (Article L. 1121-1 du Code du travail) et un transfert de charges que je ne suis pas tenu(e) d'accepter contractuellement. De plus, je ne souhaite pas exposer mes données personnelles aux risques de sécurité liés à un usage mixte, ni assumer la responsabilité de la sécurité des données usagers sur un terminal grand public non sécurisé par vos soins.

Par conséquent, je suis au regret de vous informer que je ne procéderai pas à l'installation de l'application e-CPS sur mon téléphone personnel.

Je reste à votre entière disposition pour effectuer ces démarches dès que vous m'aurez confié un terminal mobile professionnel sécurisé, ou tout autre moyen d'authentification (carte physique et lecteur) fourni par l'établissement.

Dans cette attente, l'impossibilité d'accéder aux services numériques (DUI, MSSanté) ne saurait m'être imputée comme une faute, s'agissant d'une carence de fourniture de matériel imputable à l'employeur.

Je vous prie d'agréer, Monsieur le Directeur, l'expression de mes salutations distinguées.

Copie : Section syndicale FO, Inspection du Travail.

CONCLUSION

La numérisation de l'action sociale ne doit pas se faire sur le dos des salariés. Le passage au RPPS+ et l'usage de la e-CPS sont des évolutions techniques qui structurent désormais notre métier. Cependant, l'outil ne doit jamais devenir une contrainte financière ou une menace pour la vie privée du travailleur.

La position de la Fédération Nationale de l'Action Sociale FO est claire : **sans matériel professionnel fourni, pas d'e-CPS.**

Nous invitons tous les syndicats à se saisir de ce dossier technique pour en faire un levier de revendication politique : la reconnaissance de la technicité de nos métiers passe aussi par l'attribution d'outils de travail dignes de ce nom, financés par les fonds publics prévus à cet effet. Ne signez rien, n'installez rien sans garantie. La protection de votre vie privée est un droit fondamental, la fourniture de l'outil de travail est un devoir patronal.

Document élaboré par le service juridique de la FNAS FO - Janvier 2026.