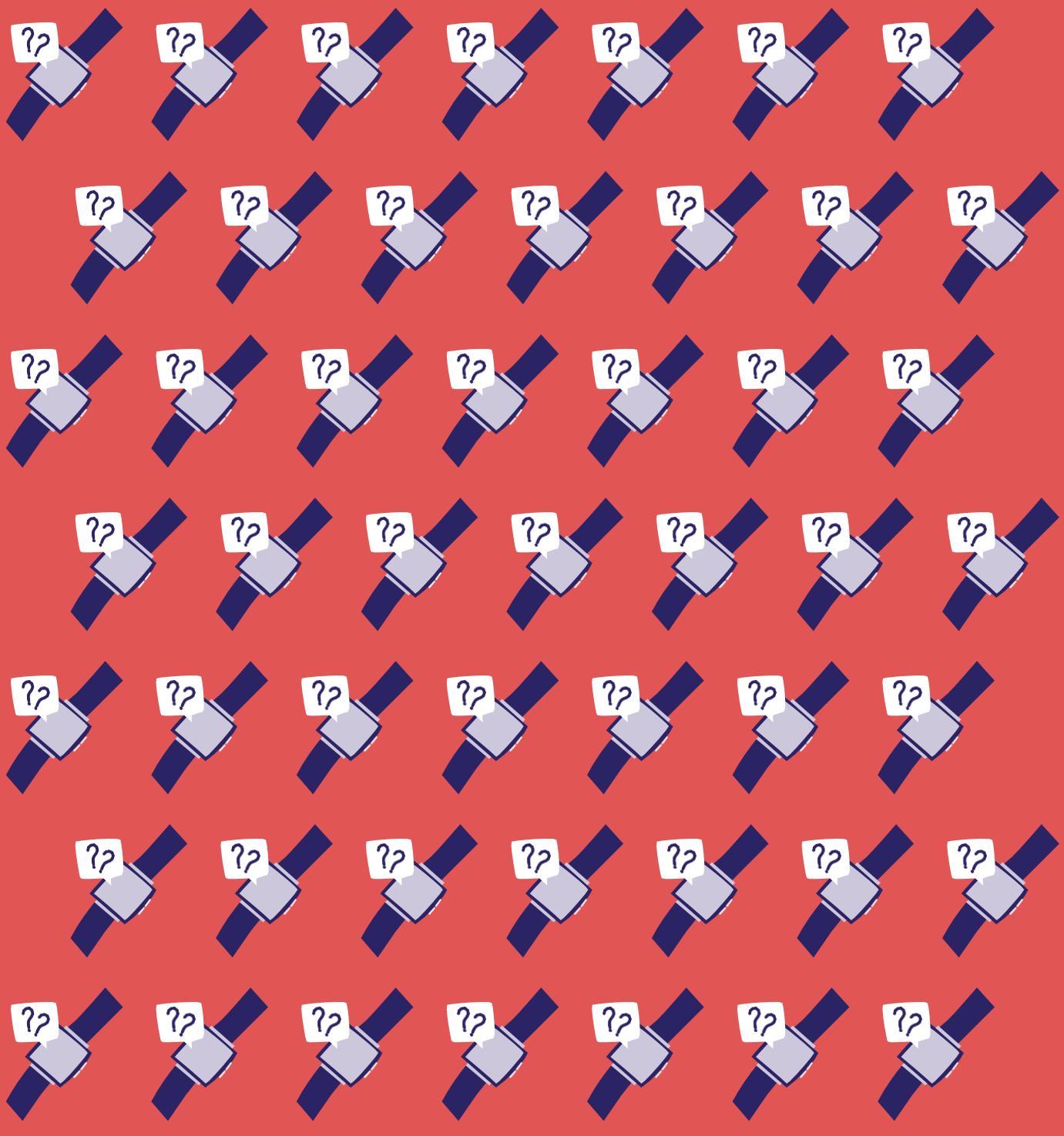
CHAPITRE 5

ADOPTER LES BONS USAGES



Une fois les services disponibles, l'entreprise doit être attentive à leur bon usage en les adaptant aux besoins réels de l'entreprise et en réduisant l'exposition à des risques en matière de sécurité (intrusion informatique, fraude, etc.).

VÉRIFIER LES FACTURES DES FOURNISSEURS

Les factures des opérateurs réunissent de nombreuses données (nombre, typologie et durée des appels, options et services souscrits, remises, etc.).

Vérifiez l'exactitude de vos factures, en particulier les premières factures émises après la signature du contrat.

À savoir : pour les professionnels, les factures détaillées de téléphonie ne comportent pas les derniers chiffres des numéros appelés depuis un poste utilisé par un salarié afin d'en préserver la confidentialité.

ADAPTER LES SERVICES AUX BESOINS DE CHACUN

L'entreprise soucieuse de réduire **ses coûts liés aux télécommunications** devra s'assurer de la réalité **du besoin et mettre en rapport les bénéfices des services souscrits et leur coût.**

→ **Par exemple, le transfert** d'appel vers un mobile est **pratique mais peut se révéler** coûteux, l'entreprise payant l'appel entrant vers le mobile.

Une mesure simple également consiste à utiliser **les services de restriction d'appel en fonction des besoins métier : appels internationaux, option d'itinérance sur les mobiles, accès aux numéros surtaxés**, etc. L'évolution des besoins de l'entreprise peut vous conduire à modifier les points de **vigilance et les paramètres de restrictions.**

Le suivi de la consommation par la lecture détaillée des factures rend compte de l'usage réel des moyens **de communication utilisés pour** l'activité de l'entreprise et permet d'adapter son offre.

→ **Les opérateurs et certains fournisseurs spécialisés pro-** posent des outils d'analyse des **données de facturation et de** trafic de l'entreprise permettant d'en extraire des graphes et des tableaux synthétiques qui facilitent la compréhension des usages, et des probables fluc-

Cela permet d'identifier facilement **des services sous ou non-utilisés.**

Communiquez sur les bonnes pratiques pour la maîtrise des dépenses de télécommunication (par exemple lors des déplacements à l'étranger) auprès des salariés.

Pour les mobiles donnez à vos **employés des conseils pour éviter la casse, la perte ou le vol et** communiquez-leur les procédures à suivre lorsque de tels événements **se produisent (voir plus** loin). Vous pouvez aussi fournir **des équipements de protection pour prémunir la dégradation du matériel.**

En cas d'usage intensif d'un terminal mobile, privilégiez les équipements à faible DAS*, et incitez à l'utilisation d'un kit main libre.

DIFFUSER LES BONNES PRATIQUES EN MATIÈRE DE SÉCURITÉ

Les moyens de télécommunications constituant un des principaux liens vers l'extérieur, ils exposent l'entreprise à des risques **en matière de sécurité : fraude, vol** de données, etc. Ce risque s'est par **ailleurs accru avec la convergence entre les télécommunications et** l'informatique classique.

Il est important de sensibiliser les différents utilisateurs de télécommunication dans l'entreprise aux bonnes pratiques en matière de sécurité :

- changement régulier des mots de passe d'accès aux services et aux **équipements,**
- mise à jour des logiciels de **sécurité,**
- identification et interdiction des usages à risque, etc.

Des prestataires (notamment **opérateurs, intégrateurs/installateurs, cabinets de conseil) peuvent vous accompagner dans cette** démarche.

Vous pouvez vous référer à des **guides de bonnes pratiques existants en matière de cybersécurité.**

Les systèmes téléphoniques étant également susceptibles d'être l'objet de piratage, **certaines règles sont à suivre afin de les sécuriser.**

PERTE ET VOL D'EQUIPEMENTS MOBILES

Les équipements mobiles, en particulier les smartphones, pré · sentent un risque particulier en raison des possibilités avérées de perte et de vol.

Ils peuvent contenir des données importantes pour l'entreprise.
Donnez des consignes de sécu**- rité en la matière, pour protéger** l'accès aux données (ex : retour **automatique en veille avec code de sécurité pour réactiver le mobile)** et n'oubliez pas le cas échéant vos obligations de notification vers les autorités compétentes (ANSSI, ou **CNIL).**

Donnez à vos employés la procé**-** dure à suivre en cas de perte ou **de vol pour en faire la déclaration dans les meilleurs délais, auprès de** l'opérateur ou du responsable de la flotte dans l'entreprise en fonction de l'organisation retenue.

Il est possible, avec certains mobiles, ou certains logiciels dits de « mobile management », de faire **bloquer le mobile, de le localiser**
et même dans certains cas d'effa**-**
cer les contenus professionnels à **distance.**

Dans tous les cas l'opérateur est **en mesure de suspendre la ligne** si vous lui communiquez le code
IMEI (à repérer dans la documenta**-** tion à la livraison).