

La protection des données au sein de l'Union européenne

Les perceptions des contrôleurs de données

Résumé

Terrain: janvier 2008

Rapport: février 2008

Ce sondage a été commandité par la direction générale de la justice, de la liberté et de la sécurité (Unité C5: protection des données) et a été coordonné par la direction générale de la communication.

Le présent document ne représente pas le point de vue de la Commission européenne.
Les interprétations et les opinions qu'il contient n'engagent que ses auteurs.

Série Flash Eurobaromètre
#226

La protection des données au sein de l'Union européenne

-

*Les perceptions des
contrôleurs de données*

Sondage réalisé par
The Gallup Organization Hongrie
à la demande de la direction
générale de la justice, de la liberté
et de la sécurité



Coordonné par la direction générale de la
communication

Le présent document ne représente pas le point
de vue de la Commission européenne. Les
interprétations et les opinions qu'il contient
n'engagent que ses auteurs.

THE GALLUP ORGANIZATION

Table des matières

Table des matières	3
Introduction	4
Principaux résultats	6
1. Perceptions quant à la législation nationale relative à la protection des données	8
1.1 Familiarité avec les dispositions des lois nationales de protection des données	8
1.2 Évaluations par les contrôleurs de données de la législation relative à la protection des données	8
1.3 Attitudes vis-à-vis des exigences de la loi de protection des données	10
1.4 Points de vue concernant la mise en œuvre et l'interprétation de la législation.....	10
2. Pratiques internes en matière de protection des données et de transferts des données personnelles	11
2.1 L'utilisation de technologies de renforcement de la protection de la vie privée	11
2.2 Transfert de données personnelles par l'internet et mesures de sécurité y afférentes	12
2.3 Transfert de données personnelles en dehors de l'UE.....	13
3. Expériences récentes en matière de confidentialité des données et de protection des données	16
3.1 Expériences des entreprises en matière de demandes d'accès et de plaintes	16
3.2 Notices d'information sur la confidentialité des données	17
3.3 Contacts avec les autorités nationales de protection des données	18
4. L'avenir du cadre légal sur la protection des données	19
5. La protection des données dans le cadre du terrorisme international	20

Introduction

Les informations liées aux personnes, appelées «données personnelles» sont collectées et utilisées dans de nombreux aspects de la vie quotidienne. Un individu fournit des données personnelles, par exemple, lorsqu'il s'inscrit dans une salle de sport, ouvre un compte bancaire, réserve un billet d'avion ou s'inscrit sur un site web. Les données personnelles sont toutes les données identifiant un individu (une «personne concernée»), comme un nom ou un numéro de téléphone. Les données personnelles faisant aujourd'hui l'objet de collectes et d'échanges plus fréquents, une réglementation supplémentaire s'impose en matière de transferts de données.

Les lois nationales sur la protection des données exigent une bonne gestion des données de la part des entités chargées de leur traitement: les «contrôleurs de données». Cette bonne gestion inclut l'obligation de traiter les données de manière équitable et sûre, et d'utiliser les données personnelles à des fins bien définies et légitimes. Les lois nationales garantissent également une série de droits aux personnes concernées par ces données.

- le droit d'être informé du traitement des données personnelles
- la raison de ce traitement de données
- le droit d'accéder aux données, et
- (si nécessaire) le droit de modifier ou de supprimer ces données.

Ces deux dernières décennies, la protection des données au sein de l'UE a fait face à de nouveaux défis et subi de profonds changements. Ainsi, l'introduction et l'extension du marché unique et de la «société de l'information» a accru le volume de données personnelles circulant entre les États membres de l'UE. Bien que les législations nationales visent à garantir un niveau de protection identique et les mêmes droits, certaines différences existent. Ces variations pourraient faire éventuellement obstacle à la libre circulation des informations et constituer des obstacles supplémentaires pour les opérateurs économiques et les citoyens. Pour lever ces obstacles et supprimer ces contraintes, sans entamer la protection des données personnelles des citoyens, la directive 95/46/CE («directive européenne sur la protection des données»)¹ a été élaborée afin d'harmoniser les dispositions en vigueur dans ce domaine.

Le présent sondage Flash Eurobaromètre sur *la protection des données au sein de l'UE* (n° 226) vise à évaluer les perceptions des contrôleurs de données en matière de protection des données au sein des 27 États membres de l'UE. Les thèmes couverts par le présent sondage sont les suivants:

- Les perceptions quant à la législation nationale relative à la protection des données
- Les pratiques internes liées à la protection des données et au transfert de données personnelles
- Les expériences récentes en matière de confidentialité des données et de protection des données
- L'avenir du cadre légal sur la protection des données
- La protection des données dans le cadre du terrorisme international

L'échantillon du présent sondage a été sélectionné au hasard, mais de manière disproportionnée, selon deux critères: le pays et la taille de l'entreprise (20-49, 50-249, 250+). Toutes les organisations privées et non privées des secteurs NACE C-Q étaient éligibles (à l'exception de l'agriculture et de la pêche).

Le nombre de sondés principaux visé varie selon la taille de la population du pays concerné et s'élève à au moins 300 dans les États membres de l'UE les plus peuplés, à au moins 200 dans les États

¹ Directive 95/46/CE du Parlement et du Conseil du 24 octobre 1995 sur la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

membres moyennement peuplés, et au moins 100 organisations ont été sondées dans les plus petits États membres.

Le travail de terrain du présent sondage a été réalisé entre le 8 et le 16 janvier 2008. Nous avons interrogé au hasard plus de 4835 «contrôleurs de données» dans les 27 États membres de l'UE. Les points de vue exprimés dans le présent document ont été formulés par les personnes identifiées comme responsables de la protection des données au sein des organisations participantes. Le sondage ciblait les personnes suivantes au sein des organisations, dans l'ordre de préférence suivant: les responsables de la protection des données, les responsables informatiques, les directeurs de ressources humaines, les responsables du marketing et, si une entreprise ne comptait aucune de ces fonctions, le directeur général. L'entretien a été mené avec le directeur, identifié par un tiers et/ou par lui-même comme étant la personne en charge de la protection des données au sein de l'organisation.

Une pondération post-stratification a été appliquée en vue de rétablir les proportions modifiées artificiellement en fonction de la taille de l'entreprise et de son secteur d'activité. Dans le cas d'estimations récapitulatives européennes ou supranationales, les entretiens sont pondérés afin de corriger la surreprésentation des pays dans l'échantillon de départ.

Ce rapport analytique présente la moyenne des résultats pour les 27 États membres de l'UE, ainsi que ceux pour chaque pays, catégorie d'entreprise (par ex. la taille de l'entreprise et son secteur d'activité) et caractéristique des répondants (par ex. la position au sein de l'entreprise). Si une question identique ou équivalente a été posée dans le cadre du précédent sondage Eurobaromètre sur la protection des données (*Flash EB 147*), il est procédé à une comparaison pour les pays concernés.

Une note technique précisant la manière dont les instituts partenaires Gallup ont réalisé le sondage est jointe à la fin du rapport analytique. Cette note détaille les méthodes d'entretien, l'échantillonnage et les marges d'erreur statistiques.

Principaux résultats

Perceptions quant à la législation en vigueur relative à la protection des données

- Une majorité de personnes responsables des questions liées à la protection des données au sein des entreprises (56 %) ont déclaré *connaître assez bien les dispositions de la loi de protection des données*. Cependant, seuls 13 % ont affirmé connaître *très bien* cette loi.
- Une proportion identique de répondants (56 %) a estimé que le *niveau de protection offert aux citoyens par leur loi nationale de protection des données* est «moyen». Vingt-huit pour cent ont déclaré que le niveau de protection était «élevé» et seuls 11 % l'ont qualifié de «faible».
- La moitié des répondants au sein de l'UE estiment que la *législation ne peut faire face à la quantité grandissante d'échanges d'informations personnelles*. Seuls 5 % des répondants ont estimé que la législation en vigueur en matière de protection des données était tout à fait adaptée.
- Les personnes responsables des questions liées à la protection des données ont généralement formulé une *évaluation positive des exigences des lois de protection des données*: 91 % se sont déclarés plutôt d'accord avec l'affirmation selon laquelle les exigences de la loi de protection des données sont nécessaires afin de respecter un niveau élevé de protection des consommateurs et les droits fondamentaux des citoyens, seuls 35 % ont estimé que les exigences de la loi de protection des données sont trop strictes et 28 % ont estimé que les exigences de la loi de protection des données ne sont pas nécessaires, sauf pour certains secteurs d'activité.
- En ce qui concerne la *mise en œuvre et l'interprétation des lois nationales de protection des données au sein de l'UE*, les avis sont partagés: 38 % estiment que l'harmonisation de la loi de protection des données des États membres est suffisante pour permettre la libre circulation des données personnelles au sein de l'UE, tandis que 33 % ne partagent pas ce point de vue; un tiers (33 %) estime que la loi de protection des données est interprétée et appliquée de façon plus rigoureuse dans leur pays que dans les autres États membres, alors qu'un quart (25 %) affirme le contraire.
- Une part significative des répondants n'ont pas été à même de juger de l'adéquation de l'harmonisation des lois de protection des données des États membres (29 %) ou ont jugé extrêmement difficile de déterminer si leur loi nationale de protection des données avait été introduite plus rigoureusement que dans d'autres États membres (42 %).

Pratiques internes en matière de protection des données et de transfert des données personnelles

L'utilisation de technologies de renforcement de la protection de la vie privée

- Environ la moitié des contrôleurs de données interrogés à travers l'UE (52 %) a déclaré utiliser des technologies de renforcement de la protection de la vie privée au sein de leur entreprise. Quatorze pour cent ont déclaré ne pas utiliser de technologies de renforcement de la protection de la vie privée et n'en avoir jamais entendu parler.

Transfert de données personnelles par l'internet

- Deux tiers des répondants au sein de l'UE (65 %) ont indiqué que leur entreprise transférait des données personnelles par l'internet. Un répondant sur trois (32 %) a admis que son entreprise ne prenait aucune mesure de sécurité lors du transfert de données personnelles par l'internet.

Transfert de données personnelles vers des pays hors UE

- Seule une minorité de répondants ont indiqué que leur entreprise transférait des données personnelles vers des pays hors UE (10 %).
- Parmi les entreprises qui ont transféré des données personnelles vers des pays hors UE, près de la moitié des répondants (46 %) ont indiqué qu'il s'agissait essentiellement de données sur les

clients ou les consommateurs pour un usage commercial, et 27 % ont déclaré qu'il s'agissait de données sur le personnel pour les besoins de gestion des ressources humaines.

- Les e-mails sont, de loin, le mode de transfert des données personnelles privilégié vers des pays hors UE; 78 % des répondants ont déclaré que leur entreprise transférait les données personnelles par e-mail.
- Parmi les répondants ayant indiqué que leur entreprise transférait des données vers des pays situés en dehors de l'UE, seul un répondant sur trois connaît l'expression «clauses contractuelles normalisées» (34 %).

Expériences récentes en matière de confidentialité et de protection des données

Expériences des entreprises en matière de demandes d'accès et de plaintes

- Près de la moitié des sondés (46 %) ont indiqué que leur entreprise avait reçu des demandes d'accès aux données personnelles l'année précédente, mais seule une minorité d'entre eux ont déclaré que leur entreprise avait reçu plus de 50 demandes.
- Seuls 3 % des répondants ont affirmé que leur entreprise avait reçu des plaintes de personnes dont les données étaient en cours de traitement.

Notices d'information sur la confidentialité des données

- Quatre répondants sur 10 au sein de l'UE (41 %) ont répondu que leur entreprise conservait et mettait à jour des notices d'information sur la confidentialité des données et 17 % des sondés ont déclaré que leur entreprise surveillait la fréquence à laquelle ces notices d'information sur la confidentialité des données étaient examinées par le public.

Contacts avec les autorités nationales de protection des données

- Au niveau de l'UE-27, 13 % des sondés ont déclaré être régulièrement en contact avec les autorités nationales de protection des données de leur pays.
- Les répondants ont majoritairement déclaré contacter les autorités nationales de protection des données de leur pays pour demander des lignes de conduite (60 %) ou pour des notifications (56 %).

L'avenir du cadre légal sur la protection des données

- Quatre répondants sur dix (38 %) ont approuvé les cinq actions énumérées en vue d'une amélioration et d'une simplification de la mise en place du cadre légal sur la protection des données. Seuls 9 % des répondants se sont déclarés favorables à une seule action ou à aucune d'entre elles.
- L'action privilégiée en vue de l'amélioration et de la simplification de la mise en place d'un cadre légal sur la protection des données est *une meilleure harmonisation des règles sur les mesures de sécurité* (84 % des répondants se sont déclarés favorables à cette action), tandis que l'action la moins plébiscitée (56 %) est l'introduction d'une *législation de protection des données spécifique à chaque secteur d'activité*.

La protection des données dans le cadre du terrorisme international

- De l'avis de la plupart des répondants, la lutte contre le terrorisme justifie la restriction des droits à la protection des données. Une majorité de répondants ont convenu qu'il devrait être possible de contrôler les données personnelles des personnes lorsqu'elles prennent l'avion (80 %), les appels téléphoniques (70 %) et l'utilisation de l'internet et des cartes de crédit (73 % et 69 %, respectivement) si ces actions servent à lutter contre le terrorisme.

- Les répondants ont toutefois mis en doute toute disposition autorisant les autorités à assouplir les lois de protection des données. La plupart des répondants, favorables à un assouplissement (tel que mentionné ci-dessus) ont répondu que cela devrait se faire dans des limites clairement définies: près de 30 % des répondants ont souligné que seules les personnes soupçonnées d'activités terroristes doivent être surveillées, tandis qu'entre 19 % et 30 % des répondants souhaitent des sauvegardes encore plus strictes, comme une supervision de ce contrôle par le pouvoir judiciaire.

1. Perceptions quant à la législation nationale relative à la protection des données

1.1 Familiarité avec les dispositions des lois nationales de protection des données

Interrogés quant à leur niveau de connaissance des dispositions des lois nationales de protection des données, la majorité (56 %) des personnes identifiées comme étant responsables des questions liées à la protection des données au sein des organisations sondées ont déclaré connaître assez bien les dispositions de la législation relative à la protection des données. Seuls 13 % ont toutefois déclaré connaître très bien cette loi. Trois répondants sur dix ont par ailleurs admis ne pas vraiment connaître les dispositions de la loi.

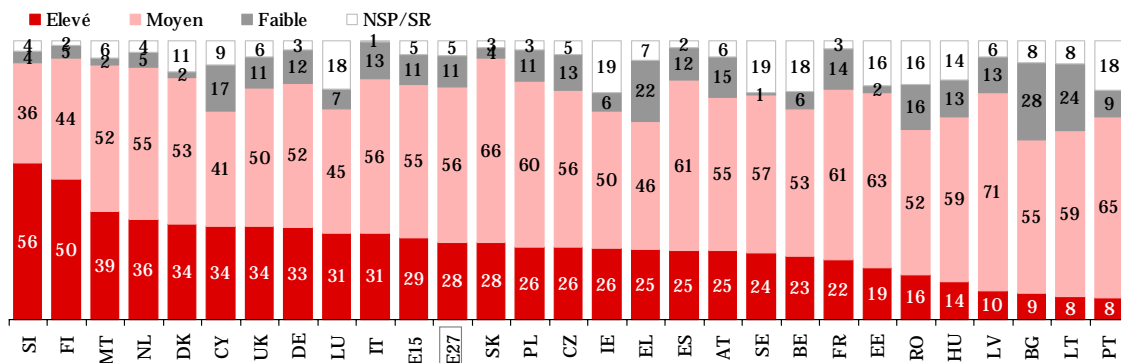
1.2 Évaluations par les contrôleurs de données de la législation relative à la protection des données

Plus de la moitié des répondants (56 %) ont qualifié de «moyen» le **niveau de protection offert aux citoyens par les lois nationales de protection des données**. Vingt-huit pour cent ont estimé que le niveau de protection était «élevé» et seuls 11 % l'ont qualifié de «faible».

Une ventilation des résultats par pays fait apparaître d'importantes disparités entre les États membres. En Slovaquie et en Finlande, une majorité de répondants a indiqué que le niveau de protection offert aux citoyens par les lois nationales de protection des données était élevé (56 % et 50 %, respectivement). En outre, 36 % des Slovaques et 44 % des Finlandais interrogés ont estimé que le niveau de protection était moyen.

Le Portugal et la Lituanie (8 % chacun) sont les pays dont les répondants ont le moins estimé que le niveau de protection était élevé. La Bulgarie et la Lettonie suivent, avec 9 % et 10 % respectivement des répondants partageant ce point de vue. Les répondants lettons ont par ailleurs été les plus susceptibles de qualifier de moyen le niveau de protection offert par leurs lois de protection des données (71 %), tandis que les répondants bulgares l'ont majoritairement qualifié de faible (28 %).

Niveau de protection offert par la loi de protection des données



Q1. Diriez-vous que le niveau de protection offert par la Loi française de Protection des Données pour les citoyens est...? % Base: tous les répondants, par pays

La moitié des répondants à travers l’UE ont estimé que la **législation n’était pas adaptée pour faire face à la quantité grandissante d’échanges d’informations personnelles**, comme celles transférées par l’internet (38 % l’ont jugée plutôt mal adaptée et 12 % pas du tout adaptée). Seuls 5 % des répondants ont estimé que la législation existante sur la protection des données était tout à fait adaptée pour faire face à l’augmentation des échanges électroniques de données et 37 % ont estimé qu’elle était plutôt bien adaptée.

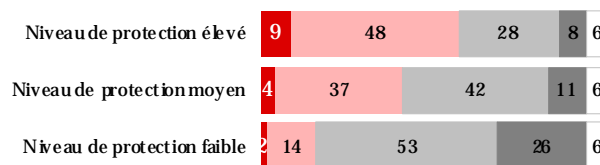
Une ventilation des résultats par pays révèle que dans six États membres seulement, une majorité de sondés indiquent que la législation existante sur la protection des données est tout à fait adaptée ou plutôt bien adaptée pour faire face à la quantité grandissante d’échanges d’informations personnelles par l’internet. Parmi ceux-ci, la Slovénie présente le taux le plus élevé, avec un total de 59 %. Le Danemark (55 %), l’Estonie (54 %), Malte et la Grèce (52 % chacun) et l’Autriche (50 %) comptent également une majorité de répondants qui estiment que la législation existante est adaptée.

Une analyse comparative des opinions formulées par les contrôleurs de données révèle une **correspondance relativement forte entre les avis** liés à la protection offerte par les lois de protection des données en vigueur et la capacité de ces lois à faire face à la quantité grandissante d’échanges d’informations personnelles. Une majorité de répondants ayant qualifié d’«élevé» le niveau de protection offert par leur loi respective ont également estimé que cette législation pouvait faire face aux volumes croissants d’informations personnelles échangées; 48 % ont estimé que la législation était plutôt bien adaptée et 9 % ont estimé que la législation était tout à fait adaptée.

La législation existante et la quantité grandissante d’échanges d’informations personnelles

par niveau de protection offert par la loi de protection des données

■ Tout à fait adaptée ■ Plutôt bien adaptée ■ Plutôt mal adaptée
■ Pas du tout adaptée □ NSP/SR



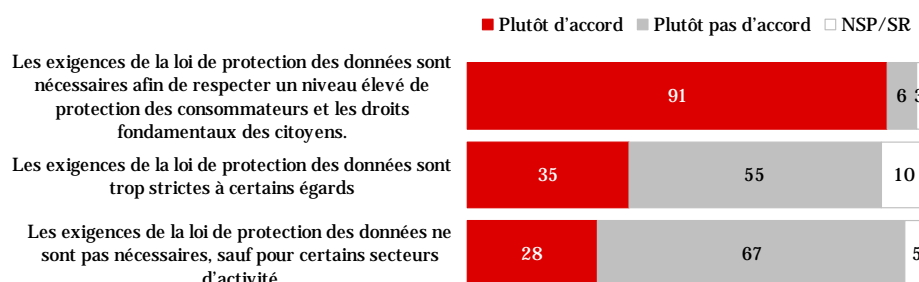
Q1. Diriez-vous que le niveau de protection offert par la Loi française de Protection des Données pour les citoyens est...?; Q4. Selon vous, pensez-vous que la législation existante sur la protection des données est adaptée ou non pour faire face à la quantité grandissante d’échanges d’informations personnelles? % Base: tous les répondants

En comparaison, ceux qui ont répondu que le niveau de protection offert par leur loi de protection des données était «faible» ont eu le plus tendance à estimer que la législation n’était pas du tout adaptée. Plus de la moitié des répondants (53 %) ont affirmé que la législation était plutôt mal adaptée pour faire face aux volumes croissants en circulation et un quart des répondants (26 %) ont déclaré que la législation n’était pas du tout adaptée.

1.3 Attitudes vis-à-vis des exigences de la loi de protection des données

De manière générale, les personnes responsables des questions liées à la protection des données ont évalué positivement les exigences des lois de protection des données. Environ 9 répondants sur 10 ont convenu que les **exigences de la loi de protection des données sont nécessaires** afin de respecter un niveau élevé de protection des consommateurs et les droits fondamentaux des citoyens. Seuls 35 % des répondants ont estimé que les **exigences de la loi de protection des données sont trop strictes** et 28 % ont estimé que les **exigences de la loi de protection des données ne sont pas nécessaires**, sauf pour certains secteurs d'activités. Ces évaluations positives démontrent que les responsables des questions liées à la protection des données ne s'opposent pas à ce type de législation. Ils semblent au contraire vivement soutenir sa mise en œuvre.

Opinions concernant les exigences de la loi de protection des données



Q2. D'après votre expérience commerciale et de façon générale, seriez-vous plutôt d'accord ou plutôt pas d'accord avec chacune des phrases relatives aux exigences de la loi de protection des données ?
%, Base: tous les répondants

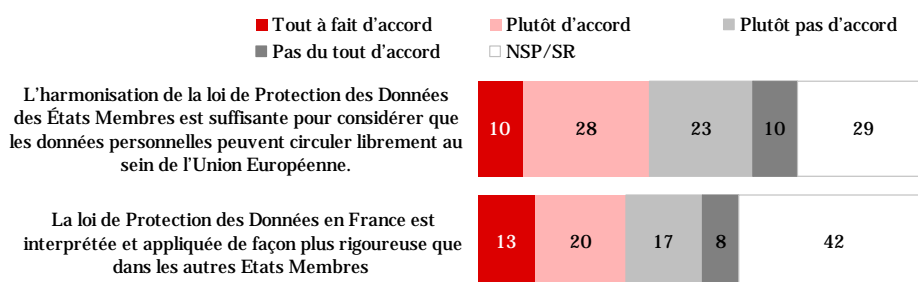
1.4 Points de vue concernant la mise en œuvre et l'interprétation de la législation

En ce qui concerne la mise en œuvre et l'interprétation des lois nationales de protection des données à travers l'UE, les avis divergent. Trente-huit pour cent des répondants sont d'accord avec l'affirmation selon laquelle **l'harmonisation des lois de protection des données des États membres est suffisante** pour considérer que les données personnelles peuvent circuler librement au sein de l'UE, par rapport aux 33 % qui ne partagent pas ce point de vue. Au niveau de l'UE-15, la part des répondants estimant que les lois de protection des données sont suffisamment harmonisées (pour permettre la libre circulation des données personnelles au sein de l'UE) a légèrement augmenté entre 2003 et 2008 (46 % en 2003 contre 50 % en 2008; soit +4 points de pourcentage).

Interrogés quant à l'interprétation et à l'application des lois de protection des données au sein des États membres, 33 % ont affirmé que la **loi de protection des données est interprétée et appliquée de façon plus rigoureuse** dans leur pays que dans les autres États membres, tandis qu'une part plus faible des répondants a déclaré le contraire (25 %). En réponse à cette question également, la proportion des répondants partageant ce point de vue a légèrement augmenté entre 2003 et le sondage actuel (62 % en 2003, 65 % en 2008).

Un groupe non négligeable de répondants n'a pas été à même de juger du niveau d'harmonisation des lois de protection des données des États membres (29 %) ou ont jugé difficile de déterminer si leur loi nationale de protection des données avait été introduite de manière plus rigoureuse que dans les autres États membres (42 %).

Opinions concernant l'application de la loi de protection des données



Q3. Pour chacune des propositions suivantes, dites moi si vous êtes tout à fait d'accord, plutôt d'accord, plutôt pas d'accord ou pas du tout d'accord avec elles ?
%, Base: tous les répondants

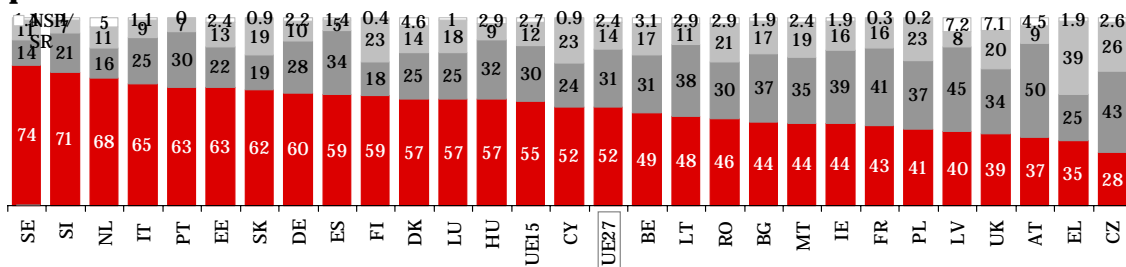
2. Pratiques internes en matière de protection des données et de transferts des données personnelles

2.1 L'utilisation de technologies de renforcement de la protection de la vie privée

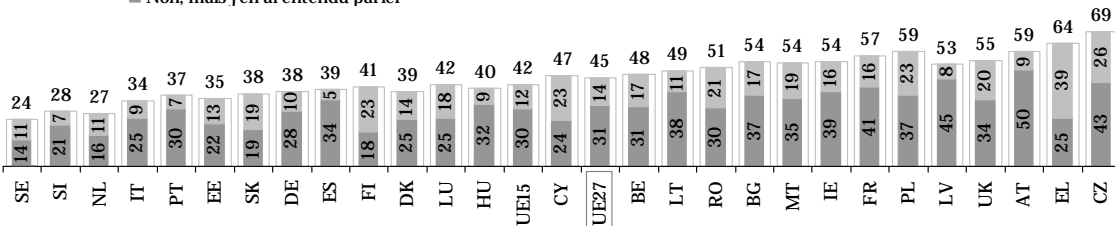
Environ la moitié des contrôleurs de données interrogés à travers l'UE (52 %) ont déclaré utiliser des technologies ou logiciels améliorant la confidentialité des bases de données de leur entreprise (à savoir des technologies de protection de la vie privée). Trois répondants sur 10 (31 %) ont déclaré ne pas utiliser ce type de technologie au sein de leur entreprise, tout en en connaissant l'existence, tandis que 14 % ont déclaré ne pas utiliser de technologies de protection de la vie privée car ils n'en ont jamais entendu parler. Par rapport à l'utilisation de ces technologies en 2003, la proportion des entreprises ayant utilisé ces technologies a sensiblement augmenté au sein des États membres de l'UE-15 (passant de 32 % à 55 %).

Une ventilation des résultats par pays fait à nouveau apparaître une forte variation; alors que trois quarts des entreprises suédoises ont déclaré utiliser des technologies de renforcement de la protection de la vie privée (74 %), à peine plus d'un quart des entreprises tchèques ont affirmé y recourir (28 %). Une analyse du pourcentage de répondants ayant déclaré que leur entreprise n'utilise pas de technologies de renforcement de la protection de la vie privée révèle que la moitié des répondants autrichiens n'utilisent pas ces technologies bien qu'ils aient déjà entendu parler de ces logiciels et technologies (et peut-être de leurs bénéfices également). Les répondants grecs ont, en revanche, été les plus susceptibles de ne pas recourir aux technologies de renforcement de la protection de la vie privée car ils n'en ont jamais entendu parler (39 %).

Utilisation des technologies de renforcement de la protection de la vie privée



■ Non, et je n'en ai jamais entendu parler
■ Non, mais j'en ai entendu parler



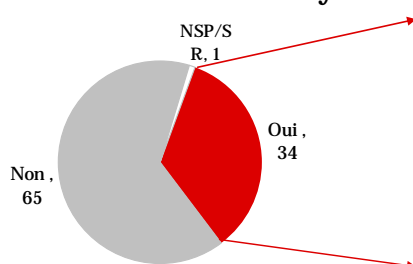
Q5. Utilisez-vous des technologies ou des logiciels améliorant la protection des bases de données dans votre entreprise, aussi appelés 'technologies de renforcement de la protection de la vie privée'? (par exemple, éliminateurs de cookies, outils de cryptage, logiciel assurant l'anonymat automatique, plateforme pour les préférences de confidentialité (P3P))
%, Base: tous les répondants, par pays

Les répondants travaillant dans le secteur des services ont été plus susceptibles que les répondants d'autres *secteurs d'activités* de recourir aux technologies de renforcement de la protection de la vie privée. Cinquante-neuf pour cent des répondants du secteur des services ont affirmé ne pas utiliser de technologies de renforcement de la protection de la vie privée, par rapport notamment aux 47 % enregistrés par les répondants du secteur du commerce. Une ventilation des résultats selon la *taille de l'entreprise* révèle que l'utilisation des technologies de renforcement de la protection de la vie privée est plus répandue dans les grandes entreprises, comptant plus de 250 employés (70 %). 47 % des répondants issus des plus petites entreprises et 58 % de ceux issus des moyennes entreprises ont déclaré utiliser ces technologies.

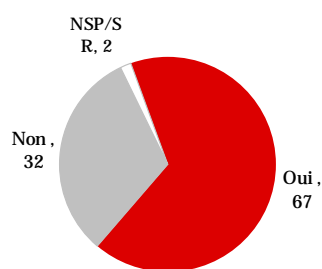
2.2 Transfert de données personnelles par l'internet et mesures de sécurité y afférentes

Deux tiers des répondants à travers l'UE (65 %) ont indiqué que leur entreprise transférait des données personnelles par l'internet. Deux tiers des entreprises transférant des données par l'internet (67 %) ont également pris des mesures pour améliorer la sécurité des données transférées. 32 % des répondants ont néanmoins reconnu que leur entreprise ne prenait aucune mesure de sécurité lors du transfert de données personnelles par l'internet.

Transfert des données personnelles via Internet et mesures de sécurité y afférentes



Q6. Votre société transmet-elle des données personnelles via Internet ?
%, Base: tous les répondants



Q7. Prenez-vous de quelconques mesures pour améliorer la sécurité des données que vous transférez ?
%, Base: ceux qui transfèrent des données personnelles par l'internet

La proportion des entreprises ayant transféré des données personnelles par l'internet varie entre 13 % en Allemagne et 59 % en Slovaquie. En analysant les autres pays situés en tête et en queue de classement, on constate qu'en Bulgarie (14 %), au Luxembourg (22 %) et aux Pays-Bas (23 %), moins d'un répondants sur quatre a déclaré que son entreprise transférait des informations personnelles par l'internet, en comparaison avec une majorité de répondants au Portugal (58 %), au Danemark (56 %) et en Autriche (50 %).

Les entreprises des secteurs de la construction et de la fabrication (38 % et 37 %, respectivement) ont été plus susceptibles d'avoir transféré des données personnelles par l'internet que celles des secteurs des services et du commerce (33 % et 30 %, respectivement). Mais lorsque les entreprises du secteur des services ont transféré des données par l'internet, elles ont été plus susceptibles (que celles d'autres secteurs) d'avoir pris des mesures pour préserver la sécurité des données (73 % par rapport à 63 % dans le secteur de l'exploitation minière et d'extraction, et 64 % dans les secteurs de la construction et du commerce).

Bien que les plus grandes entreprises aient transféré un nombre à peine supérieur de données personnelles par l'internet, elles ont pris davantage de mesures pour préserver la sécurité de ces données. Trente-sept pour cent des répondants issus des grandes entreprises ont déclaré transférer des données personnelles par l'internet, et 86 % d'entre eux ont également indiqué que des mesures étaient prises pour améliorer la sécurité des données. À titre de comparaison, 33 % des répondants issus des petites entreprises ont déclaré que des données étaient transférées par l'internet et 61 % d'entre eux ont également affirmé que des mesures de sécurité étaient prises.

2.3 Transfert de données personnelles en dehors de l'UE

L'un des principes de la *directive européenne relative à la protection des données* veut que les données personnelles puissent uniquement être transférées vers des pays hors UE qui garantissent un niveau de protection *approprié*. Seule une minorité de répondants européens responsables des questions liées à la protection des données ont indiqué que leur entreprise transférait des données personnelles vers des pays hors UE (10 %), contre 89 % qui ont indiqué n'opérer aucun transfert de ce type.

Les secteurs de l'exploitation et des services ont été plus enclins à transférer des données personnelles vers des pays non européens, avec respectivement 13 % et 10 % des répondants déclarant que leur entreprise procédait à ce type de transfert. À titre de comparaison, 5 % des répondants issus du secteur de la construction et 6 % des répondants du secteur du commerce ont répondu que ces données étaient transférées en dehors de l'UE.

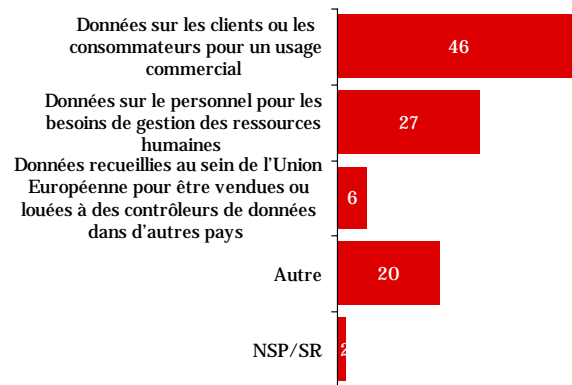
Une ventilation des résultats par *taille de l'entreprise* révèle que les plus grandes entreprises affichent le taux de répondants le plus élevé ayant répondu que les données personnelles étaient transférées en dehors de l'UE (15 % contre 9 % des petites entreprises, et 11 % des moyennes entreprises). La perspective plus internationale des grandes entreprises en comparaison avec celle des PME peut expliquer cette différence.

Les répondants ayant indiqué que leur entreprises transférait également des données personnelles vers des pays hors UE ont également été interrogés sur: a) le type de données personnelles qu'ils transféraient le plus fréquemment, et b) les canaux étaient utilisés pour transférer ces données. Il a enfin été demandé aux répondants s'ils connaissaient l'expression «clauses contractuelles normalisées».

Type de données transférées vers des pays hors Union européenne

Parmi les entreprises ayant transféré des données personnelles vers des pays hors UE, près de la moitié des répondants (46 %) ont indiqué qu'il s'agissait essentiellement de données sur les clients ou les consommateurs pour un usage commercial, et 27 % ont déclaré qu'il s'agissait de données sur le personnel pour les besoins de gestion des ressources humaines. 6 % ont affirmé que leur entreprise transférait essentiellement des données européennes destinées à être vendues ou louées à des contrôleurs de données dans d'autres pays. Enfin, un cinquième des répondants a répondu que leur entreprise transférait essentiellement des données autres que celles susmentionnées.

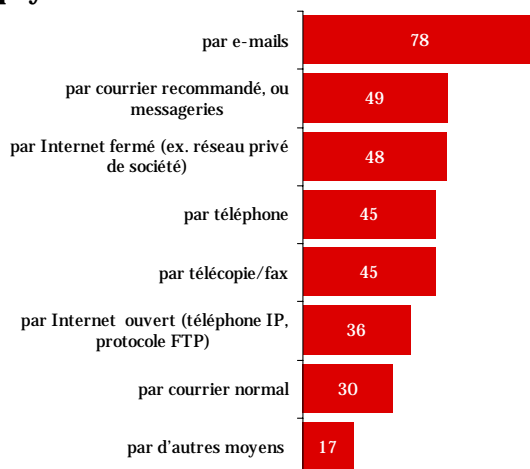
Type de données transférées vers des pays hors UE



Q9. Quel type de données votre entreprise transfère-t-elle à de tels pays, principalement?
% Base: ceux qui transfèrent des données vers des pays hors UE

Canaux utilisés pour le transfert de données personnelles vers des pays situés en dehors de l'UE

Modes de transfert des données personnelles vers des pays hors UE



Q10. Comment votre société transfère-t-elle des données personnelles vers d'autres pays? Utilisez-vous chacun des outils que je vais vous citer? Transférez-vous des données personnelles...
% Base: ceux qui transfèrent des données personnelles vers des pays hors UE

Les données personnelles sont essentiellement transférées au moyen d'outils électroniques. Quatre cinquièmes des répondants (78 %) ont déclaré que leur entreprise avait transféré des données personnelles vers des pays hors UE par e-mails. Une part plus ou moins équivalente des répondants a répondu que ce transfert se faisait par courrier recommandé ou messagerie (49 %), par Internet «fermé» (comme un réseau d'entreprise) (48 %), par téléphone ou télécopie (45 % chacun). Une part plus restreinte de répondants ont répondu que leur entreprise transférait des données personnelles vers des pays non européens par Internet «ouvert» (téléphone IP ou serveur ftp) (36 %) ou par courrier normal (30 %). Enfin, 17 %

des sondés ont signalé l'utilisation de canaux autres que ceux mentionnés pour ces transferts.
Connaissance de l'expression «clauses contractuelles normalisées»

La directive européenne relative à la protection des données impose aux États membres d'autoriser les transferts de données personnelles vers des pays situés en dehors de l'UE à la condition qu'ils garantissent une protection appropriée de ces données. La Commission européenne a approuvé des «clauses contractuelles normalisées», que les entreprises transférant des données vers des pays hors UE peuvent utiliser pour respecter les dispositions de la directive relative à la protection des données. Il a été demandé aux répondants ayant indiqué que leur entreprise transférait des données vers des pays hors UE s'ils connaissaient l'expression «clauses contractuelles normalisées». Seul un tiers des répondants (34 %) connaît cette expression et deux tiers (65 %) ont déclaré n'en avoir jamais entendu parler.

3. Expériences récentes en matière de confidentialité des données et de protection des données

3.1 Expériences des entreprises en matière de demandes d'accès et de plaintes

L'«accès de la personne concernée» est le droit de la personne concernée à consulter les données conservées à son propos par une organisation. S'il est prouvé que les informations personnelles relatives à la personne concernée sont erronées ou trompeuses, des mesures peuvent être prises afin de rectifier ou de détruire ces informations. Dans des cas extrêmes, un dédommagement peut être réclamé en cas de dommages et de détresse. Afin d'analyser les expériences des entreprises européennes en matière de demandes d'accès et de plaintes déposées par les personnes concernées, il a été demandé aux répondants:

- combien de **demandes d'accès** leur entreprise a reçues l'année précédente, et
- s'ils ont déjà reçu des **plaintes** de personnes dont les données personnelles étaient en cours de traitement.

Près de la moitié des sondés responsables des questions liées à la protection des données au sein de leur entreprise (46 %) ont indiqué que leur entreprise avait reçu des demandes d'accès aux données personnelles au cours de l'année précédente.

Un peu moins de quatre répondants sur 10 (37 %) ont déclaré que leur entreprise n'a reçu aucune demande d'accès au cours de la même période. Enfin, dix-sept pour cent des répondants n'ont pas pu préciser / ignoraient si leur entreprise avait reçu des demandes d'accès.

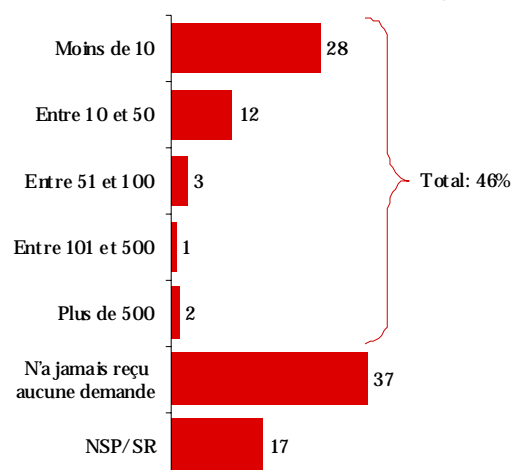
Les personnes invitées à donner accès aux données personnelles détenues par leur entreprise étaient les plus susceptibles de déclarer quelques demandes seulement: 28 pour cent des répondants ont déclaré que leur entreprise avait reçu moins de 10 demandes, et 14 % ont indiqué que leur entreprise avait reçu entre 10 et 50 demandes. Seuls 6 % des sondés ont répondu que leur entreprise avait reçu plus de 50 demandes au cours de l'année précédente.

De manière générale, **seuls 3 % des répondants ont répondu que leur entreprise avait reçu des plaintes** de personnes dont les données étaient en cours de traitement.

Une ventilation des résultats selon les *caractéristiques des entreprises* révèle que les personnes responsables des questions liées à la protection des données au sein des entreprises de plus de 250 employés sont celles ayant reçu le plus de demandes d'accès et de plaintes. Les répondants issus des plus grandes entreprises ont, sans grande surprise, déclaré avoir reçu un nombre élevé de demandes d'accès (13 %, plus de 50 demandes) – tandis que seuls 5 % et 6 %, respectivement, des répondants issus des petites et moyennes entreprises ont déclaré avoir reçu plus de 50 demandes.

De même, le pourcentage de répondants ayant déclaré que leur entreprise avait reçu des *plaintes* de personnes dont les données étaient en cours de traitement s'élève à 14 % dans les plus grandes entreprises, comparé à 3 % au sein des moyennes entreprises et 2 % dans les plus petites entreprises.

Demandes d'accès aux données personnelles conservées par l'organisation



Q14. Pourriez-vous indiquer le nombre approximatif de demandes d'accès à des données personnelles reçues par votre entreprise au cours de l'année précédente?
%, Base: tous les répondants

Par rapport à 2003, le nombre de plaintes reçues reste stable au sein des pays de l’UE-15 (4 % en 2003 contre 3 % en 2008), mais les demandes d’accès sont en chute libre (passant de 71 % à 46 %).

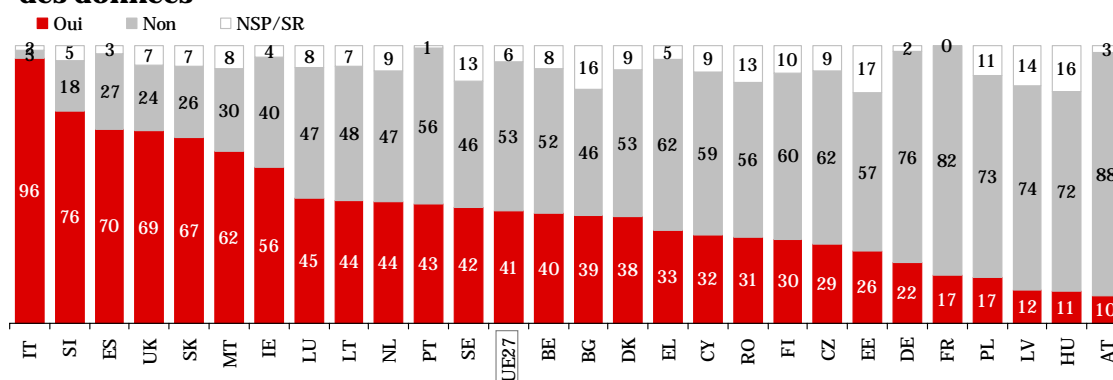
3.2 Notices d’information sur la confidentialité des données

Une notice d’information sur «la confidentialité des données» décrit comment un contrôleur de données collecte des informations personnelles sur les personnes concernées; par exemple, la notice mentionne quelles informations personnelles sont collectées, comme les données peuvent être utilisées, avec qui ils peuvent les partager, quels choix les personnes concernées ont quant à leur utilisation, et comment les données sont protégées. Un contrôleur de données peut mettre à jour la notice d’information sur la confidentialité des données lorsque des modifications sont apportées aux pratiques de confidentialité, en raison de modifications apportées aux exigences légales ou réglementaires pertinentes et d’application, au niveau de l’entreprise ou de ses pratiques.

Quatre répondants sur 10 au sein de l’UE (41 %) ont répondu que leur entreprise **conserve et met à jour des notices d’information sur la confidentialité des données**, tandis qu’à peine moins de la moitié des répondants ont déclaré que ce n’était pas le cas (53 %). Une minorité de 6 % ignorait si leur compagnie mettait par à jour ces notices d’information.

Les résultats par pays révèlent que presque tous les répondants en Italie ont déclaré que leur entreprise conservait et mettait à jour une notice d’information sur la confidentialité des données (96 %). La Slovaquie (76 %), l’Espagne (70 %), le Royaume-Uni (69 %), la République tchèque (67 %), Malte (62 %) et l’Irlande (56 %) affichent également une majorité de répondants ayant déclaré que leur entreprise mettait à jour ces notices. Les entreprises autrichiennes, par contre, ont le moins souvent déclaré conserver et mettre à jour des notices d’information sur la confidentialité des données (10 % des répondants ont répondu «oui»), suivies des entreprises hongroises (11 %) et lettones (12 %).

Conserver et mettre à jour des notices d’information sur la confidentialité des données



Q13a. Votre société conserve-t-elle et met-elle à jour des notices d’information sur la confidentialité des données ?
%, Base: tous les répondants, par pays

Dix-sept pour cent des sondés au sein de l’UE-27 ont répondu que leur **entreprise surveillait la fréquence à laquelle leur notice d’information sur la confidentialité des données est examinée par le public**, et trois quarts (74 %) ont déclaré que leur entreprise ne surveillait pas ces pratiques. En outre, 9 % des répondants ignoraient si leur entreprise procédait à cette surveillance.

Les entreprises italiennes sont celles qui ont non seulement conservé et mis à jour le plus fréquemment une notice d’information sur la confidentialité des données, mais elles ont également été les plus susceptibles de déclarer surveiller l’examen par le public de ces notices (65 % ont déclaré que c’était le cas en Italie). La proportion des entreprises ayant surveillé la fréquence à laquelle les notices étaient examinées par le public est largement inférieure dans tous les autres États membres.

Les entreprises du secteur des services ont déclaré, plus souvent que celles d’autres *secteurs d’activité*, qu’elles mettaient à jour et conservaient des notices d’information sur la confidentialité des données et surveillaient à quelle fréquence ces notices étaient examinées par le public. La moitié des répondants

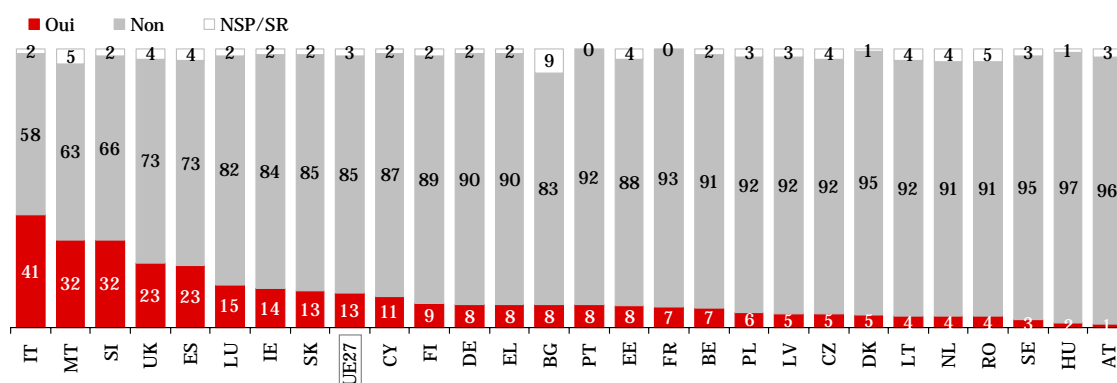
dans le secteur des services (49 %) ont répondu que leur entreprise mettait à jour des notices d'information sur la confidentialité des données, par rapport notamment aux 33 % seulement dans le secteur de la construction. De même, un répondant sur cinq travaillant dans le secteur des services (19 %) a répondu que son entreprise surveillait l'examen par le public des notices d'information contre, par exemple, 12 % dans le secteur du commerce.

Une ventilation des résultats selon la *taille de l'entreprise* révèle que celles comptant moins d'employés sont moins susceptibles que les plus grandes entreprises de conserver et mettre à jour des notices d'information sur la confidentialité des données ou de surveiller à quelle fréquence ces notices sont examinées par le public. Trente-six pour cent des répondants issus des entreprises comptant moins de 50 employés ont mis à jour les notices d'information sur la confidentialité des données, et 15 % ont déclaré surveiller si ces notices étaient examinées par le public. Les pourcentages correspondants de répondants dans les entreprises de plus de 250 employés s'élèvent à 62 % et 27 %.

3.3 Contacts avec les autorités nationales de protection des données

Au niveau de l'UE-27, 13 % des sondés ont déclaré être en contact régulier avec les autorités nationales de protection des données de leur pays, tandis que 85 % ont affirmé le contraire. Les résultats révèlent de fortes variations entre pays au niveau de la régularité des contacts avec les autorités de protection des données. Les entreprises italiennes sont les plus susceptibles d'être régulièrement en contact avec les autorités concernées (41 %). Un pourcentage élevé de répondants est également en contact régulier avec les autorités nationales de protection des données à Malte et en Suède (chacun 32 %). Des contacts réguliers avec les autorités de protection des données sont pratiquement inexistantes en Autriche (seul 1 % des répondants ont déclaré être en contact régulier avec les autorités concernées), en Hongrie (2 %) et en Suède (3 %).

Contacts avec les autorités nationales de protection des données



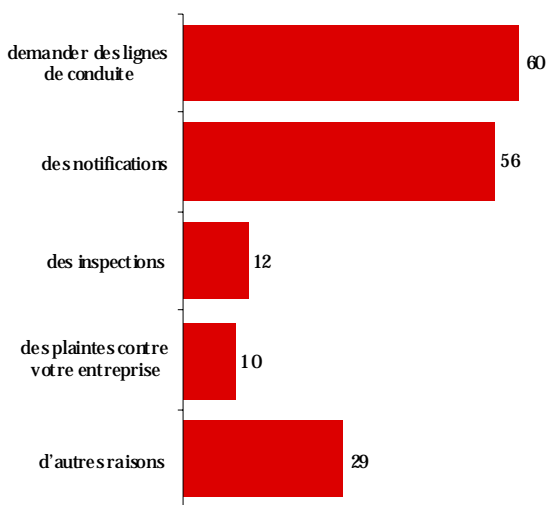
Q12a. Etes-vous en contact régulier avec les autorités nationales de protection des données de France ?
%, Base: tous les répondants, par pays

Une ventilation des résultats par *secteur d'activité* révèle que les contrôleurs de données dans le secteur des services sont plus susceptibles que ceux d'autres secteurs d'être en contact régulier avec les autorités nationales de protection des données (18 % contre 10 % dans le secteur de l'exploitation 8 % dans les secteurs de la construction et du commerce). La probabilité qu'une entreprise ait des contacts réguliers avec les autorités nationales de protection des données augmente proportionnellement à la *taille de l'entreprise*. Les répondants travaillant dans une grande entreprise sont trois fois plus susceptibles que ceux des plus petites entreprises de déclarer être en contact régulier avec les autorités de protection des données (31 % contre 10 %).

Il a également été demandé aux répondants pourquoi ils avaient contacté les autorités nationales de protection des données. Ils ont pu opter pour plusieurs motifs dans une liste prédéfinie.

Les répondants ont majoritairement (60 %) déclaré être à la recherche de lignes de conduite. Plus de la moitié des répondants (56 %) ont contacté ces autorités pour des notifications. Des proportions plus restreintes de répondants ont déclaré avoir contacté les autorités concernant des inspections (12 %) ou des plaintes contre leur entreprise (10 %). Enfin, trois répondants sur 10 (29 %) ont déclaré avoir été en contact avec leurs autorités de protection des données pour d'autres raisons que celles mentionnées dans le sondage.

Motif des contacts avec les autorités nationales de protection des données



Q12h. Avez-vous été en contact avec les autorités nationales de protection des données pour...
%, Base : ceux qui ont contacté les autorités nationales de protection des données

4. L'avenir du cadre légal sur la protection des données

Dans ce chapitre, nous analysons les actions auxquelles les entreprises seraient favorables en vue d'une amélioration et d'une simplification de la mise en place du cadre légal sur la protection des données. Les répondants avaient le choix parmi une liste de cinq actions et il leur a été demandé d'indiquer pour chacune de celles-ci s'ils y étaient favorables ou non.

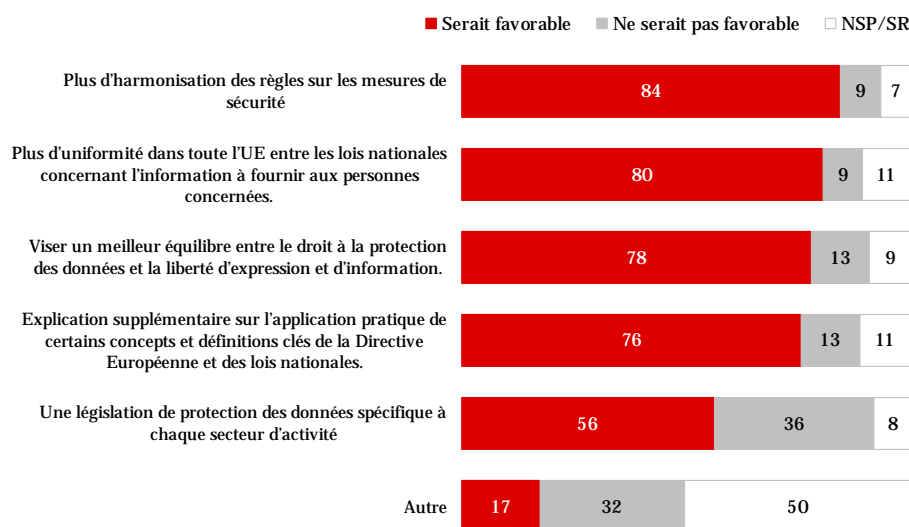
L'action privilégiée en vue d'une amélioration et d'une simplification de la mise en place du cadre légal sur la protection des données est une **plus grande harmonisation des règles sur les mesures de sécurité** (84 % des sondés se sont montrés favorables à cette action), tandis que l'action la moins plébiscitée est l'élaboration d'une **législation de protection des données spécifique à chaque secteur d'activité** (56 % des sondés ont privilégié cette action).

Conformément au désir d'une plus grande harmonisation, une part similaire de répondants a soutenu les autres actions énumérées dans le sondage:

- Huit répondants sur 10 se sont déclarés favorables à **une plus grande uniformité dans toute l'UE entre les lois nationales concernant l'information à fournir aux personnes concernées.**
- Soixante-dix-huit pour cent sont favorables à l'objectif **visant à un meilleur équilibre entre le droit à la protection des données et la liberté d'expression et d'information.**
- Une part légèrement inférieure (76 %) serait favorable à une **explication supplémentaire sur l'application de certains concepts et définitions clés de la directive européenne et des lois nationales.**

Enfin, 17 % des répondants se sont déclarés favorables à une action autre que celles énumérées dans le sondage, tandis que 32 % ne se sont pas montrés favorables à une quelconque action supplémentaire en vue d'une amélioration et d'une simplification de la mise en place du cadre légal sur la protection des données.

Actions privilégiées pour une amélioration et une simplification de la mise en place du cadre légal sur la protection des données



Q16. Parmi les actions suivantes, pourriez-vous indiquer celles pour lesquelles vous seriez favorable à une amélioration et une simplification de la mise en place du cadre légal sur la protection des données?
%, Base: tous les répondants

5. La protection des données dans le cadre du terrorisme international

À la fin du sondage, les contrôleurs de données ont été invités à présenter leur point de vue concernant toute restriction des droits en matière de protection des données en raison des actions de surveillance menées dans le cadre de la lutte contre le terrorisme. Il a été demandé aux répondants si, en prenant en considération le terrorisme international, il serait possible de surveiller les actions des personnes, par exemple leurs appels téléphoniques, l'utilisation qu'elles ont de l'internet, les transactions par cartes de crédit ou leurs données personnelle lorsqu'elles prennent l'avion.

Les résultats révèlent que la plupart des sondés sont prêts à accepter des restrictions des droits relatifs à la protection des données dans le cadre de la lutte contre le terrorisme. Une majorité des répondants ont répondu qu'il serait possible de surveiller les différentes actions énumérées dans le sondage (un oui conditionnel ou inconditionnel a été exprimé par 69 % à 80 % des répondants, selon l'activité), tandis que seule une minorité a totalement rejeté cette idée (16 % à 28 %).

Les répondants ont toutefois marqué un doute quant à une quelconque disposition qui permettrait aux autorités de restreindre les droits en matière de protection des données, même dans le cadre de la lutte contre le terrorisme. La plupart des répondants favorables à une surveillance des appels téléphoniques, de l'utilisation de l'internet et des cartes de crédit ou des données personnelles en cas de vol en avion ont souligné que les restrictions des droits en matière de protection des données doivent être clairement délimitées. Près de 30 % des répondants ont souligné que seules les personnes soupçonnées d'activités terroristes doivent être surveillées et entre 19 % et 30 % souhaitent même voir appliquées des règles plus strictes, à savoir la surveillance des activités des personnes soupçonnées uniquement sous la supervision d'un juge.

Surveiller les appels téléphoniques des personnes, l'utilisation qu'elles ont d'Internet, l'utilisation des cartes de crédit et les données personnelles des personnes lorsqu'elles prennent l'avion



Q17. En prenant en considération la lutte contre le terrorisme international, pensez-vous que, dans certaines circonstances, il devrait être possible de/d' :
 %, Base: tous les répondants

Plus de trois quarts (80 %) des répondants acceptent la surveillance des données personnelles des personnes lorsqu'elles prennent l'avion et un tiers (34 %) estiment que cela peut se faire sans condition (à savoir *dans tous les cas*) – cette action a bénéficié de l'appui le plus «inconditionnel».

La plupart des répondants ont partagé le point de vue des autorités publiques selon lequel l'internet est un outil efficace et dangereux pour la préparation d'attentats terroristes et qu'il doit être surveillé. Après la surveillance des données personnelles en cas de vol en avion, les répondants ont été le plus susceptibles d'accepter une surveillance de l'utilisation de l'internet (73 %), avec à peine un quart (23 %) rejetant cette possibilité.

Les répondants ont davantage hésité à accepter la surveillance des appels téléphoniques et des transactions par cartes de crédit. Si une majorité accepte cette possibilité (70 % et 69 %, respectivement, mais dans la plupart des cas sous condition), plus d'un quart des répondants se sont opposés à l'idée de ces vérifications (27 % et 28 %, respectivement). Tout particulièrement dans le cas des appels téléphoniques, les répondants craignaient que les autorités s'immiscent trop dans la vie privée sous le couvert de la lutte contre le terrorisme. Dans ce cas, les répondants ont été le moins susceptibles de déclarer que la surveillance doit être possible dans tous les cas (9 %) et le plus susceptibles de déclarer que cette mesure doit s'appliquer uniquement aux personnes soupçonnées d'activités terroristes (31 %) ou que même ces personnes doivent uniquement être surveillées sous la supervision d'un juge (30 %).