

# Accès aux voies de recours en matière de protection des données à caractère personnel dans les États membres de l'UE

## Résumé

*L'article 8 de la Charte des droits fondamentaux de l'Union européenne garantit à toute personne dans l'Union européenne (UE) le droit à la protection de ses données à caractère personnel. Il exige que ces données soient traitées loyalement et à des fins déterminées. Il garantit à toute personne le droit d'accéder aux données personnelles la concernant et d'en obtenir la rectification. Il stipule qu'une autorité indépendante doit veiller au respect de ce droit. L'article 47 garantit à toute personne le droit à un recours effectif, notamment que sa cause soit entendue équitablement, publiquement et dans un délai raisonnable.*

Les violations de la protection des données à caractère personnel peuvent avoir lieu presque partout : au travail, au supermarché ou sur internet. Elles peuvent engendrer une grande détresse émotionnelle chez les personnes qui en sont victimes et porter atteinte à leur réputation ou à leurs relations.

*« Les conséquences [de la violation du secret médical] ont été terribles. Toutes les personnes en qui j'avais confiance se sont éloignées – parents, aide à domicile, médecin. La perte de mon autonomie était en jeu. [...] C'est tout mon univers qui s'est effondré. Je me suis retrouvé seul, sans argent ni soutien. »* (Victime d'une violation de la protection des données n'ayant pas engagé de recours, Allemagne)

Les personnes ayant fait l'objet de ce type de violations ont le droit d'engager un recours. Elles peuvent se tourner vers leur autorité nationale chargée de la protection des données ou envisager d'autres alternatives possibles pour porter plainte et de demander réparation. Beaucoup engagent un recours afin d'éviter à d'autres de subir de tels préjudices ou pour faire reconnaître que leurs droits ont été bafoués. En revanche, la peur de s'engager dans des procédures trop longues, trop complexes ou trop coûteuses, notamment si elles nécessitent une représentation juridique, peut dissuader ces personnes de porter plainte. Il est

également possible que ces dernières échouent à trouver l'expertise ou les conseils qu'elles recherchent.

Ce projet de l'Agence des droits fondamentaux de l'Union européenne (FRA) fournit une analyse comparative des voies de recours possibles à l'échelle de l'UE afin de garantir les droits des personnes en matière de protection des données à caractère personnel. Il se trouve à la jonction de deux droits fondamentaux garantis par la Charte des droits fondamentaux de l'Union européenne : le droit à la protection des données à caractère personnel (article 8) et le droit à un recours effectif (article 47). Le droit à un recours effectif constitue une condition préalable au respect et à la mise en œuvre de tous les autres droits fondamentaux, y compris le droit à la protection des données. C'est pourquoi il est important de prendre simultanément en considération ces deux droits fondamentaux.

*« Je crois que le seul recours qui m'a paru motivant était de [faire] reconnaître que j'avais été lésé ou de recevoir une décision disant : "Ce qui vous est arrivé n'est pas acceptable, vos droits ont été bafoués". »* (Représentant d'une organisation de soutien aux victimes, Roumanie)

Les recherches socio-juridiques de la FRA portent sur l'utilisation et la mise en œuvre des recours ainsi que les facteurs qui entravent l'accès à des voies de recours effectifs en cas de violation de la protection des données à caractère personnel. En s'appuyant sur les preuves issues de ces recherches, la FRA recense les obstacles existants et propose des solutions permettant de les surmonter afin de contribuer à la réforme du régime de protection des données en cours dans l'UE.

Ce résumé présente les principales conclusions de la FRA, qui sont publiées intégralement dans le rapport portant sur l'accès aux voies de recours en matière de protection des données à caractère personnel dans les États membres de l'UE (*Access to data protection remedies in EU Member States*).

## Contexte juridique

La directive de l'Union européenne sur la protection des données, ou Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, garantit la disponibilité de recours en matière de protection des données dans les États membres en astreignant chaque État membre à se doter d'une autorité de contrôle indépendante.

Mue par la volonté d'améliorer l'efficacité de la mise en œuvre du droit fondamental à la protection des données à caractère personnel, la Commission

européenne a proposé en 2012 une vaste réforme des règles de l'UE en matière de protection des données à caractère personnel. Le train de réformes est constitué d'une proposition de règlement général sur la protection des données qui remplace la directive générale sur la protection des données de 1995, ainsi qu'une proposition de directive générale sur la protection des données qui remplace la décision-cadre relative à la protection des données.

Le programme de réforme proposé vise à renforcer l'indépendance des autorités nationales chargées de la protection des données et de consolider leur capacité d'action en cas de violations.

### Description et catégories des personnes interrogées

Toutes les citations du résumé sont tirées du rapport complet portant sur l'accès aux voies de recours en matière de protection des données à caractère personnel dans les États membres de l'UE (*Access to data protection remedies in EU Member States*). Par souci de lisibilité, la FRA a modifié les catégories des sources des citations. Le résumé fait ainsi référence à la catégorie « victime de violations de la protection des données n'ayant pas engagé de

recours », apparaissant dans le rapport intégral sous le terme juridique de « non-plaignant ». De même, les victimes ayant engagé un recours sont désignées dans le rapport par le terme de « plaignants ». La FRA a également interrogé des personnes travaillant au sein d'organisations de soutien aux victimes de violations de la protection des données, dont des organisations de travailleurs, des syndicats ou des organisations de plaignants. Leur rôle est précisé dans le résumé, tandis que le rapport les désigne comme des « intermédiaires ». Les « avocats » et les « juges » sont désignés comme tels dans les deux publications.

Tableau : Nombre de personnes interrogées et de participants aux groupes de discussion

	Nombre de personnes interrogées			Nombre de participants aux groupes de discussion ou aux entretiens		
	Plaignants	Non-plaignants	Juges/ procureurs	Personnel des autorités de protection des données	Intermédiaires	Avocats en exercice
<i>Minimum prévu</i>	30-40		6	6	6	6
Allemagne	20	6	5	6	5	4
Autriche	7	6	5	2	7	8
Bulgarie	16	14	8	6	2	3
Espagne	11	3	4	5	6	6
Finlande	24	6	6	8	6	6
France	25	9	5	6	7	8
Grèce	16	15	4	7	7	5
Hongrie	13	19	6	9	6	5
Italie	2	9	6	7	7	7
Lettonie	5	2	2	5	5	4
Pays-Bas	24	9	7	6	6	5
Pologne	15	15	6	8	8	6
Portugal	7	7	6	2	3	4
République tchèque	4	6	5	10	6	6
Roumanie	4	2	3	0	6	3
Royaume-Uni	28	2	6	10	9	4
<b>Total</b>	<b>351</b>		<b>84</b>	<b>97</b>	<b>96</b>	<b>84</b>

## Collecte des données et portée

Pour cette recherche, la FRA a étudié le cadre juridique en matière de protection des données dans les 28 États membres de l'UE, en analysant les lois et règles de procédure pour présenter une analyse comparative de la situation juridique en matière de protection des données à caractère personnel dans l'ensemble de l'UE.

Entre avril et septembre 2012, le réseau de recherche multidisciplinaire de la FRA, Franet, a mené une recherche qualitative sur le terrain dans 16 États membres : Allemagne, Autriche, Bulgarie, Espagne, Finlande, France, Grèce, Hongrie, Italie, Lettonie, Pays-Bas, Pologne, Portugal, République tchèque, Roumanie

et Royaume-Uni. Plus de 700 personnes appartenant à six groupes cibles ont été interrogées ou ont participé à des groupes de discussion. Ces six groupes cibles étaient : des plaignants, ou des victimes de violations de la protection des données ayant engagé un recours ; des « non-plaignants », ou des victimes présumées de violations de la protection des données ayant décidé de ne pas engager de recours ; des juges ; des membres du personnel des autorités chargées de la protection des données ; des intermédiaires, dont des membres du personnel des organisations de la société civile soutenant les personnes ayant été victimes de telles violations ; ainsi que des avocats en exercice.

## Principaux résultats et conseils fondés sur des éléments de preuve

S'appuyant sur ses résultats, la FRA entrevoit des possibilités concrètes pour les institutions, les États membres et les mécanismes de l'UE visant à la mise en œuvre des recours en matière de protection des données d'améliorer la disponibilité et la qualité des recours proposés aux victimes de violations de la protection des données dans l'UE. À la lumière de ces éléments, la FRA suggère diverses mesures pour aider les institutions de l'UE et les décideurs nationaux à développer et à mettre en œuvre des mesures qui visent à garantir la protection des données à caractère personnel et le recours en cas de violation de ces données.

### Les types de violation de la protection des données

Les résultats de recherche indiquent que les sources les plus fréquentes de violations de la protection des données sont les activités sur internet, le démarchage et la vidéosurveillance à travers l'utilisation clandestine de télévision en circuit fermé. Les organes gouvernementaux, les organes chargés de l'application de la loi ainsi que les institutions financières et sanitaires sont le plus souvent responsables de ces violations.

### Connaître ses droits : la sensibilisation

L'amélioration de l'efficacité des recours passe également par une meilleure sensibilisation du public en ce qui concerne la protection des données, la nature des violations de ce droit, les mécanismes de réparation et la manière de les utiliser. Pour engager un recours, le public doit être capable de reconnaître une violation de la protection des données à caractère personnel.

Cette recherche de la FRA a étudié les différents types de violations, l'identité de leurs auteurs et leur impact sur les victimes. Elle s'est également penchée sur ce qui motive les victimes à engager un recours.

Les violations de la protection des données les plus fréquemment mentionnées lors de la recherche sur le terrain étaient liées aux activités sur internet. Celles-ci incluent les médias sociaux, les achats en ligne, la fuite de données personnelles sur les boutiques en ligne, le piratage de comptes de messagerie et de bases de données, le vol d'identité, les failles de sécurité et l'utilisation abusive des données personnelles par les grandes entreprises d'internet. Les activités sur internet font clairement figure de territoire à hauts risques du point de vue de la protection des données.

Un autre type de violations fréquemment cité est lié au démarchage et à la prospection commerciale effectués sans le consentement du destinataire, lorsque les données personnelles sont utilisées de manière abusive sur les téléphones mobiles, par courrier électronique ou postal. La recherche sur le terrain suggère que les opérateurs de téléphonie mobile et les agents de recouvrement sont souvent responsables de ces violations. Les personnes interrogées notent également des pratiques

frauduleuses telles que la vente de données personnelles à des tiers.

Les personnes interrogées déclarent souvent avoir été filmées à leur insu dans le cadre d'une vidéosurveillance sur leur lieu de travail, dans la sphère publique ou au supermarché. Dans différents pays, plusieurs personnes interrogées ont indiqué avoir été surveillées à leur insu par les autorités publiques au moyen de technologies spéciales ou de systèmes de télévision en circuit fermé installés en secret. Plusieurs autorités de protection des données, par exemple au Royaume-Uni, ont élaboré des lignes directrices relatives à l'utilisation de la télévision en circuit fermé.

Les personnes interrogées ont également mentionné d'autres violations supposées de la protection des données, caractéristiques de la relation employeur-employé. Parmi celles-ci figurent : la collecte des données personnelles de l'employé, l'accès aux données personnelles stockées sur les ordinateurs appartenant à l'employeur, l'utilisation de badges et de système de positionnement universel (GPS), l'utilisation discriminatoire de données personnelles sensibles collectées par le biais de sondages et d'audits, et la divulgation des données personnelles de l'employé par l'employeur.

D'après la recherche empirique, les violations financières, dont le piratage de comptes bancaires ou de cartes de crédit, sont également assez fréquentes. Malgré ces informations, la recherche n'a identifié que peu de plaignants déclarant avoir subi des pertes financières à la suite de ces violations. Dans nombre de ces cas, les personnes interrogées qualifient les sommes concernées de mineures ; il s'agit de montants liés à des communications téléphoniques, à des frais postaux et aux frais nécessaires pour accéder à leur dossier et le modifier.

## Impact sur les victimes

Les personnes interrogées décrivent le préjudice causé par les violations de la protection des données comme étant de nature sociale et psychologique, telles une détresse émotionnelle ou une atteinte à la réputation. Des préjudices financiers sont aussi mentionnés, mais moins fréquemment.

Les personnes qui ont subi des violations de la protection des données demandent réparation pour de nombreuses raisons, par exemple pour obtenir la rectification ou la suppression de leurs données à caractère personnel ou afin que des sanctions soient appliquées à l'encontre des auteurs. Les répondants ont également déclaré vouloir éviter que d'autres personnes subissent de telles violations dans le futur et obtenir la reconnaissance que leur droits ont été bafoués.

Lorsqu'ils sont interrogés sur les préjudices causés par la violation de la protection de leurs données, plaignants et non-plaignants ont recours à un vocabulaire psychologique ou social. Ils mettent l'accent soit sur leurs émotions, soit sur le préjudice causé à leurs relations ou à leur réputation. Ils évoquent, à des degrés variables, la détresse émotionnelle, l'insécurité et l'outrage, notamment le sentiment de persécution, voire de désespoir, et l'impression d'être surveillé en permanence. Ils expliquent le préjudice porté à leur réputation professionnelle ou personnelle, une perte de confiance et d'autres formes de préjudice moral, comme l'a montré la recherche de terrain réalisée par la FRA, par exemple, en Allemagne, en Autriche, en Bulgarie, en Espagne, en Grèce, en Hongrie, en Italie, en Lettonie, aux Pays-Bas ou en Pologne. Un plaignant espagnol décrit l'un des aspects de cette sensation comme « une impuissance face à un abus de pouvoir ».

*« Mon départ [de mon travail] a été très douloureux. [...] J'en avais mal au cœur [...] et je ne pouvais pas me défendre parce que j'ignorais si ces accusations étaient réelles. »* (Victime d'une violation de la protection des données ayant porté plainte, Grèce)

Les personnes interrogées en Italie, aux Pays-Bas, au Portugal, en République tchèque et en Roumanie signalent des dommages causés par les violations dans le domaine de l'emploi : procédures disciplinaires, suspensions et/ou cessations de l'emploi, ou encore risque de renvoi. Dans certains de ces cas, les préjudices impliquent des pertes financières, dont le fait de manquer une opportunité en matière d'emploi, de ne pas pouvoir obtenir un prêt, de ne pas avoir droit à des soins de santé ou à des avantages, le coût élevé d'une représentation juridique ou des pertes financières immédiates, ainsi que la perspective de pertes financières causées par des hypothèses illégitimes concernant leurs responsabilités.

Certaines personnes interrogées cherchent réparation surtout pour rétablir leur situation personnelle. D'autres, bien plus nombreuses, veulent éviter que d'autres personnes subissent de telles violations dans le futur, obtenir la reconnaissance de la violation ou qu'il y soit mis un terme, ou encore obtenir la sanction de leur auteur. L'obtention d'une compensation financière ne figure pas parmi les raisons principales des demandes de réparation. Les personnes interrogées ont le plus souvent parlé de « prévenir de futures violations de droits », de « sensibiliser le public », de « mettre un terme à de mauvaises pratiques », de « défendre les droits fondamentaux », de « donner une leçon aux [autorités concernées] », d'« obtenir une reconnaissance de la violation de la part d'une autorité compétente » ou de « sanctionner les auteurs ».

Tandis que les personnes interrogées soulignent un manque de sensibilisation au problème des violations de la protection des données parmi les

professionnels comme parmi les victimes, divers États membres de l'UE possèdent également des programmes de sensibilisation.

#### Avis de la FRA

*Il existe chez les victimes un manque de sensibilisation concernant les violations de la protection des données et les recours possibles. Ces résultats, issus de la recherche empirique réalisée par la FRA, confirment les conclusions de recherches existantes menées par l'agence.*

*Comme le reconnaissait le rapport de la FRA sur La protection des données à caractère personnel dans l'Union européenne (2010), la sensibilisation aux législations relatives à la protection des données est une mission importante pour les institutions concernées, telles que les autorités nationales chargées de la protection des données. Le même manque de sensibilisation a été souligné dans le rapport de la FRA L'accès à la justice en cas de discrimination (2012) et dans l'avis de la FRA sur les directives de l'UE sur l'égalité (2013), en lien avec la législation de l'UE en faveur de la non-discrimination. Des mesures sont nécessaires pour sensibiliser l'ensemble de la population, du grand public jusqu'aux juges. Il convient d'améliorer dans l'ensemble de l'UE la publicité des organisations de soutien vers lesquelles peut se tourner un plaignant qui souhaite déposer une plainte pour violation de la protection des données personnelles.*

*L'UE pourrait promouvoir des campagnes de sensibilisation au niveau des États membres et leur octroyer un éventuel soutien financier. Afin de mieux sensibiliser les professionnels nationaux aux règles de protection des données à caractère personnel, la FRA a élaboré avec le Conseil de l'Europe et la Cour européenne des droits de l'homme un Manuel de droit européen en matière de protection des données à caractère personnel.*

*Les États membres pourraient envisager la possibilité de prendre les mesures nécessaires afin de renforcer la sensibilisation du public en ce qui concerne l'existence et le fonctionnement des modes de plainte disponibles, notamment les autorités de protection des données. De plus, les autorités de protection des données devraient veiller tout particulièrement à développer auprès de leur public leur image de gardiennes indépendantes du droit fondamental à la protection des données personnelles, et devraient intensifier leurs activités de sensibilisation sur les questions relatives à la protection des données.*

## Engager un recours : renforcer les autorités de protection des données

Les autorités de protection des données se sont révélées être la voie à suivre la plus populaire – et bien souvent la seule voie pertinente – pour les personnes demandant réparation dans les cas de violations de la protection des données. Pour pouvoir répondre à cette demande, ces entités doivent être en mesure de proposer un service solide et complet.

La directive sur la protection des données de 1995 établit les pouvoirs des autorités de protection des données, les habilitant à enquêter et à intervenir afin d'empêcher que des violations aient lieu. Elles jouent un rôle majeur dans le cadre des recours en cas de violations de la protection des données, fonctionnant souvent comme le premier point de contact pour les victimes de telles violations. Ce rôle est souvent reconnu par les tribunaux nationaux. En Finlande, par exemple, procureurs et tribunaux ont l'obligation de fournir à l'autorité de protection des données la possibilité d'être entendue dans le cadre d'affaires traitant de conduites contraires à la loi finlandaise relative aux données à caractère personnel.

## Renforcer le rôle des autorités de protection des données

Certaines des principales critiques formulées par les intermédiaires à l'égard des autorités de protection des données portent sur leur manque de communication et de transparence, ainsi que l'insuffisance de leur action en matière de sensibilisation du public. Certaines remettent également en cause l'indépendance de ces autorités, principalement à cause d'éventuelles nominations politiques.

De leur côté, les membres du personnel des autorités de protection des données soulèvent la question de la mise en application des décisions des autorités, liée à leurs compétences limitées en ce qui concerne la mise en œuvre de ces décisions, notamment le traitement illégal de données par les administrations publiques. Selon les représentants des autorités nationales chargées de la protection des données, le manque de ressources humaines et financières affecte la qualité de leur travail et entrave le fonctionnement des recours dans la pratique.

Les autorités de protection des données peuvent publier des directives afin de rectifier certaines violations de la protection des données ou d'imposer

des amendes, bien que leur capacité d'engager des recours à l'encontre de telles violations et que l'étendue de l'utilisation de ces pouvoirs varient grandement selon les États membres. Leurs prérogatives incluent les avertissements formels, les directives spécifiques, les injonctions, la révocation de permis, les amendes, d'autres sanctions financières ou le renvoi de l'affaire soit devant les tribunaux concernés, soit entre les mains du procureur compétent.

*« Parfois, les gens se plaignent de la procédure de médiation. C'est le cas lorsque les gens ignorent ce que sont réellement les objectifs d'une procédure de médiation et les limites qui sont les nôtres. Bien sûr, nous expliquons alors que "nous ne pouvons pas aller sur place et, par exemple, couper les câbles des caméras vidéos." Oui, donc, parfois, il y a simplement une incompréhension en ce qui concerne la procédure, et il faut alors que l'affaire passe devant les tribunaux. »* (Membre du personnel de l'autorité de protection des données, Autriche)

Dans la plupart des États membres de l'UE, les autorités judiciaires peuvent imposer des sanctions pénales qui prennent la forme d'amendes ou d'emprisonnement. L'éventail de durée des condamnations et du montant des amendes varie selon les États membres de l'UE. Pour certaines personnes interrogées dans le cadre de la recherche sociale sur le terrain, dans les faits, des juges exerçant en Grèce, la sévérité des sanctions contribue à l'efficacité des procédures judiciaires.

Bien que les autorités de protection des données aient normalement un certain nombre de mesures à leur disposition, elles ont le plus souvent recours à des amendes ou à des sanctions financières dans le cas de violations de la protection des données, comme le rapportent 19 États membres de l'UE. La législation nationale définit souvent le montant de l'amende imposée et de nombreux États membres de l'UE font la distinction entre personnes physiques et entités juridiques ou personnes morales. Les amendes peuvent souvent être augmentées afin de sanctionner les récidivistes, ou dans les cas où de nombreuses violations ont été commises.

*« Les principales critiques ne concernent pas notre manque d'indépendance, mais le fait que la protection des données ne soit pas efficace. Lorsque des plaignants échouent dans le cadre de demandes de réparation, ils disent : "Oubliez la protection des données." Nous avons l'image d'un tigre édenté, d'un tigre de papier. [...] C'est pour cette raison que le pouvoir de publier des directives était important pour nous ; parce que ce qui compte, c'est d'obtenir des résultats et de les faire appliquer, et non uniquement d'émettre des sanctions financières. »* (Membre du personnel de l'autorité chargée de la protection des données, Allemagne)

L'adoption du règlement proposé par la Commission européenne permettrait d'inscrire dans le droit de l'UE le pouvoir de ces autorités d'imposer des

sanctions administratives, à savoir des amendes et d'autres sanctions financières. Bien que la majorité des autorités de protection des données disposent déjà de ce pouvoir, les conclusions de la FRA montrent que le règlement proposé permettrait d'augmenter de manière significative la possibilité de recourir à des amendes plus importantes, jusqu'à un maximum de 1 000 000 EUR, ou de 2 % du chiffre d'affaires global annuel d'une entreprise.

## Engager un recours via les autorités de protection des données

La majorité des plaignants dans les 16 États membres de l'UE couverts par la recherche ont choisi d'engager un recours via l'autorité nationale chargée de la protection des données. C'est également l'option préférée de ceux qui ont envisagé d'engager un recours mais qui, pour une raison ou une autre, ont décidé de ne pas poursuivre leur action. Les plaignants déclarent avoir choisi l'autorité de protection des données plutôt que d'autres alternatives pour de nombreuses raisons, dont : coûts moindres, procédures moins longues et moins complexes, possibilité pour les personnes ne disposant pas de représentation légale d'avoir recours à cette procédure, conseils reçus, compétence des autorités et limitation de la disponibilité des autres procédures.

Les plaignants interrogés étaient plus réticents à engager des procédures judiciaires à cause des coûts plus élevés, des procédures plus longues, ainsi que du besoin ressenti d'être représenté ou assisté par un avocat. Les mesures de droit pénal jouent un rôle dans certains cas, mais ne sont que rarement utilisées dans les États membres de l'UE couverts par la recherche, hormis quelques exceptions notables.

*« Sur le moment, je n'ai pas pensé à une réparation ou à un dédommagement. J'étais mécontent de voir qu'une entreprise qui reçoit vos données puisse s'imaginer pouvoir en faire n'importe quoi. Je voulais que cette pratique cesse. Je voulais que mes données soient effacées. »* (Victime d'une violation de la protection des données ayant engagé un recours, Lettonie)

Le choix des modes de recours dépend des informations disponibles, qui sont généralement insuffisantes, et des conseils reçus. En se basant sur leur sensibilisation à ces questions, on peut diviser les personnes ayant fait l'expérience de violations de la protection des données en deux groupes. La majorité des personnes interrogées déclarent manquer d'informations. Le deuxième groupe, une minorité de personnes « bien informées », déclare disposer de suffisamment d'informations du fait de leur parcours professionnel, généralement dans le domaine juridique, ou d'expériences passées.

## Avis de la FRA

*Les autorités de protection des données, en tant que principaux acteurs défendant le droit à la protection des données, jouent un rôle crucial dans le traitement de la très vaste majorité des plaintes relatives à la protection des données. Des actions supplémentaires s'imposent afin de garantir un réel accès à ces autorités dans la pratique.*

*L'indépendance des autorités de protection des données doit être renforcée par une réforme de la législation de l'UE. Elles devraient disposer de compétences et de pouvoirs accrus, bénéficier de ressources humaines et financières adéquates, notamment d'un éventail de professionnels chevronnés, tels que des spécialistes des technologies de l'information compétents et des avocats qualifiés.*

*Le Parlement européen et le Conseil de l'Union européenne proposent un règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Ce règlement général sur la protection des données a pour but d'harmoniser la législation en matière de protection des données et de renforcer les capacités des autorités de protection des données en ce qui concerne les recours en cas de violation.*

*Le renforcement de la protection des données pourrait passer par des garanties concernant l'application des décisions des autorités ainsi que la durée raisonnable des procédures (voir également dans le contexte spécifique de la non-discrimination le rapport de la FRA L'accès à la justice en cas de discrimination dans l'UE – Vers une plus grande égalité, 2012). Cela permettrait aux autorités de protection des données de rester le point de contact privilégié en cas de violations de la protection des données, tout en rationalisant les voies de recours existantes et en réduisant les coûts totaux, les délais et les formalités (voir l'Avis de la FRA concernant le programme de réforme des règles en matière de protection des données à caractère personnel, 2012).*

*Afin de renforcer leur autorité et leur crédibilité, les autorités de protection des données devraient jouer un rôle important dans l'application du système de protection des données, en ayant le pouvoir de prononcer des sanctions ou d'engager des procédures pouvant aboutir à des sanctions (voir également le rapport de la FRA La protection des données à caractère personnel dans l'Union européenne : le rôle des autorités nationales chargées de la protection des données, 2010).*

*Cet avis est en accord avec les résultats dans le contexte d'autres organes non judiciaires, tels que les organismes responsables des questions d'égalité, comme le souligne l'avis 1/2013 de la FRA sur les directives de l'UE en matière d'égalité (p. 3) :*

*« La mesure dans laquelle les procédures de plaintes jouent leur rôle de mécanisme de réparation des dommages et de mécanisme de dissuasion pour les auteurs de violations dépend de la capacité des organes de règlement des différends à infliger des sanctions effectives, proportionnées et dissuasives. » et « permettre aux organisations de la société civile, notamment aux organismes de promotion de l'égalité, d'intenter des actions en justice ou de mener des enquêtes [...] pourrait contribuer à faciliter l'application du droit. »*

*Les autorités de protection des données sont invitées à être plus transparentes ainsi qu'à communiquer de manière efficace avec le grand public en fournissant les informations nécessaires et en facilitant l'accès aux voies de recours dans la pratique. De plus, comme le souligne le rapport de la FRA de 2010 sur le rôle des autorités chargées de la protection des données dans l'UE, ces dernières « doivent encourager une coopération plus étroite et une synergie avec d'autres gardiens des droits fondamentaux [...] dans l'architecture émergente des droits fondamentaux de l'UE » (p. 9). De telles mesures permettront d'améliorer l'image des autorités de protection des données, leur efficacité et leur indépendance telles qu'elles sont perçues, ainsi que la confiance du grand public.*

## Rallier des soutiens : renforcer le rôle des organisations de la société civile

Dans le travail mené sur le terrain, les organisations de la société civile se sont révélées être une source importante d'information, de conseil, d'assistance et de représentation juridique. Elles enrichissent de manière significative le cadre statutaire de la protection des données à caractère personnel. Elles mènent également une action de sensibilisation, notamment en ce qui concerne les questions de protection des données et les recours possibles.

Il existe cependant trop peu d'organisations de ce genre, un facteur qui limite dans la pratique l'accès du public aux voies de recours proposées.

Les résultats de la recherche réalisée sur le terrain montrent que rares sont les organisations de la société civile qui développent leur image auprès de la population dans le domaine de la protection des données, et qui sont capables de proposer des services complets et suffisamment diffusés auprès du public, ce qui limite dans la pratique l'accès de ce dernier aux voies de recours proposées.

« Avec nos partenaires, nous donnons des conseils dans différents domaines : juridique, fiscal, le meilleur achat à faire et même, de manière confidentielle, lorsqu'ils nous disent qu'ils ont des soucis, nous essayons de les informer sur leurs droits et sur les instruments juridiques à leur disposition pour résoudre ces problèmes. Parfois, nous optons plutôt pour le recours, en particulier le recours collectif depuis son entrée en vigueur, quand une question peut se révéler d'intérêt pour plusieurs personnes physiques. » (Représentant d'une organisation de soutien aux victimes, Italie)

Pendant la recherche sur le terrain dans les 16 États membres de l'UE, la FRA a éprouvé des difficultés à trouver des représentants d'organisations de la société civile ou des intermédiaires à interroger. Dans la plupart des pays, trouver des représentants d'organisations qui traitent spécifiquement des questions de protection des données, qui apportent un soutien aux victimes de violations ou qui ont une vaste expérience en la matière était un vrai défi.

Les intermédiaires interrogés dans le cadre de la recherche sur le terrain déclarent surtout fournir

à des personnes qui ont subi une violation concernant la protection de leurs données des conseils et des informations sur leurs droits et sur les recours disponibles. Ils assistent ces personnes dans le cadre de leur plainte. Parmi les autres activités mentionnées par les répondants figurent l'enseignement, la recherche et la formation. Certains mettent l'accent sur le travail de sensibilisation via des campagnes dans les médias, des articles et des publications, de même que des activités de surveillance et de lobbying.

« Notre priorité est d'informer. À travers le magazine, le site web, les médias et les différentes publications, nous donnons des explications sur de nombreuses questions, dont [la protection des données]... La deuxième chose, c'est que nous donnons des conseils aux personnes qui cherchent des informations et sont intéressées. Elles reçoivent des explications sur leurs droits et sur les procédures. Ensuite, si besoin, nous renvoyons les dossiers vers les autorités compétentes. [...] Plus tard vient la représentation juridique : on nous accorde le droit essentiel de représenter les consommateurs. » (Représentant d'une organisation de soutien aux victimes, Bulgarie)

#### Avis de la FRA

Le rapport souligne l'importance des organisations intermédiaires en tant que source d'informations, de conseils, d'assistance et de représentation juridiques. Cependant, seul un nombre très limité d'organisations de la société civile sont à même de proposer des services complets pour les victimes de violations de la protection des données. L'UE et les États membres devraient augmenter le financement des organisations de la société civile et des organes indépendants qui sont en mesure d'assister ces victimes qui engagent des recours.

Les victimes sont souvent réticentes à intenter une action en justice. Permettre à des organisations de la société civile de mener des actions devant un tribunal ou de conduire des enquêtes peut constituer une étape importante vers une meilleure application du droit. Comme cela a déjà été mis en évidence dans d'autres rapports et avis de la FRA, et confirmé par les résultats du présent rapport, les règles strictes régissant la qualité pour agir empêchent les organisations de la société civile de jouer un rôle plus direct dans les actions en justice en cas de violations des droits fondamentaux (voir le rapport de la FRA L'accès à la justice en Europe : présentation des défis à relever et des opportunités à saisir (2011) et L'accès à la justice en cas de discrimination dans l'UE - Vers une plus grande égalité (2012)).

L'Avis de la FRA concernant le programme de réforme des règles en matière de protection des données à caractère personnel (2012) signale notamment que l'UE devrait envisager d'assouplir davantage les règles sur la qualité pour agir afin de permettre aux organisations agissant dans l'intérêt public de porter plainte dans des cas où il est peu probable que les victimes intentent une action judiciaire à l'encontre d'un responsable du traitement des données, en raison du coût, de la stigmatisation et d'autres difficultés auxquelles elles seraient exposées. Comme le souligne la FRA dans ses rapports sur l'accès à la justice, cela permettrait également de garantir que les cas d'importance stratégique soient traités, ce qui renforcerait la culture d'application de la législation relative à la protection des données. Un tel élargissement des exigences en matière de la qualité pour agir devrait être accompagné de garanties additionnelles pour préserver le juste équilibre entre l'accès effectif aux voies de recours et les litiges abusifs. La Commission a proposé une forme de recours collectif représentatif dans le règlement général sur la protection des données.



## Éliminer les obstacles : réduire les coûts et alléger la charge de la preuve

La recherche de la FRA a tenté d'identifier les facteurs qui empêchent les victimes de violations de la protection des données d'engager un recours. Outre le manque de conseils et de soutien spécialisé, elle a découvert un certain nombre d'obstacles, dont les coûts, la durée excessive des procédures et les difficultés à satisfaire aux exigences de la charge de la preuve, notamment pour les violations liées à internet.

Les personnes interrogées estiment que les coûts, qu'ils soient liés aux procédures ou à la représentation juridique, constituent un obstacle important à l'accès aux voies de recours dans le domaine de la protection des données. Des procédures longues et dont les résultats sont incertains ont tendance à faire monter les coûts, ce qui veut parfois aussi dire que les coûts dépassent tout bénéfice potentiel.

Les plaignants, les intermédiaires et les avocats en exercice interrogés ont tendance, plus fréquemment que les juges interrogés, à définir la charge de la preuve comme un problème. Ils évoquent des difficultés à fournir des preuves suffisantes et complètes, notamment en ce qui concerne les activités sur internet.

De façon sans doute prévisible, les personnes physiques victimes de violations ont tendance à préférer les voies de recours qui n'impliquent pas de coûts. Les résultats de la recherche empirique révèlent que les coûts et les risques financiers figurent parmi les principales préoccupations des personnes dans leur choix d'intenter un recours puis d'y donner suite.

Le coût d'une représentation juridique, par exemple, a souvent dissuadé les victimes de violations de la protection des données de donner suite à une plainte. Au vu de l'importance d'une assistance juridique dans les affaires de protection des données, la disponibilité d'une assistance juridique gratuite et l'accès à un tel service jouent un rôle clé dans la décision de s'engager sur telle ou telle voie de recours. L'aide juridique et d'autres moyens qui rendent les modes de réparation gratuits favorisent l'accès du plus grand nombre à des tels mécanismes. Les résultats de la recherche soulignent un accès limité aux modes de réparation dû à la restriction de l'assistance juridique.

« Les plaignants sont prêts à entreprendre toutes les démarches possibles (intenter une action pénale ou civile, réclamer une indemnité, s'adresser à la Cour suprême) sous réserve qu'aucun frais n'y soit associé. Mais lorsque cela engendre des coûts, tout ce qu'ils acceptent de faire, c'est de solliciter l'Agence espagnole de la protection des données, malgré ses limites, car cette procédure est gratuite. » (Avocat, Espagne)

Lorsqu'une représentation juridique n'est pas obligatoire, les plaignants peuvent réduire les coûts de manière considérable en se représentant eux-mêmes. Une autoreprésentation n'est cependant pas toujours souhaitable, du fait de la complexité de ce domaine de la législation. Cela donne toutefois à des plaignants qui, autrement, ne l'auraient pas fait, l'opportunité d'intenter une action en justice.

La préoccupation relative au coût élevé des procédures judiciaires a également été rapportée. Ce point empêche souvent les plaignants de s'adresser aux tribunaux, même s'ils pourraient être dédommagés en obtenant gain de cause. Dans de nombreux États membres de l'UE étudiés, les personnes interrogées jugent que les frais élevés engendrés dans le cadre d'une procédure civile, y compris les frais de justice, constituent un problème ; c'est le cas, par exemple, en Allemagne, en Autriche, en Espagne, en France, en Grèce, en Hongrie, en Italie, aux Pays-Bas, en Pologne, au Portugal, et au Royaume-Uni.

« Dans le cadre d'une procédure civile, vous avez un avocat, mais peu d'avocats connaissent bien cette loi. Mais s'il vous faut un avocat, une procédure civile est tout simplement trop chère. [...] Une telle procédure peut facilement coûter quelques milliers d'euros, et c'est beaucoup. » (Juge, Pays-Bas)

Un autre obstacle à la poursuite d'actions en justice est la charge de la preuve. La plupart des plaignants interrogés dans les 16 États membres couverts par la recherche mentionnent les difficultés dont ils ont fait l'expérience pour fournir des preuves suffisantes et complètes. Les plaignants interrogés en Espagne, en Grèce, en Lettonie, au Portugal, en Roumanie et en République tchèque signalent la charge de la preuve comme étant un obstacle au fait d'engager un recours dans le domaine de la protection des données. Les problèmes sont principalement liés à la difficulté de fournir des preuves des violations de la protection des données, notamment en ce qui concerne les activités sur internet et plusieurs obstacles pratiques liés à l'obtention de preuves dans le domaine spécifique de la protection des données. Les avocats et les intermédiaires partagent cette opinion, tandis que les juges, par exemple au Portugal et en Roumanie, considèrent que la charge de la preuve est acceptable.

Avis de la FRA

*Les victimes de violations de la protection des données se voient dissuadées de poursuivre des actions en justice pour plusieurs raisons, dont les coûts et les difficultés associés à l'apport de preuves de ces violations. Les États membres de l'UE devraient envisager la promotion de mesures de soutien via des centres de conseil juridique ou du bénévolat. Ces mécanismes de soutien devraient venir compléter un système d'assistance juridique financé de manière adéquate, et non s'y substituer.*

*« Très peu de professionnels du barreau se spécialisent dans la protection des données. » (Avocat, Royaume-Uni)*

Le manque de représentation légale et de conseils d'experts accessibles, la durée et le caractère chronophage des procédures ainsi que les coûts associés peuvent dissuader les personnes victimes de violations de la protection des données de poursuivre une action en justice. Des procédures complexes, une sensibilisation insuffisante et un soutien non spécialisé peuvent également démotiver les individus et les empêcher d'engager des recours dans les cas de violations de la protection des données.

## Fournir des conseils : améliorer l'expertise juridique en matière de protection des données

La recherche montre qu'il existe un manque d'expertise au sein des professions juridiques dans le domaine de la protection des données à caractère personnel. L'insuffisance de conseils avisés prodigués par des experts, s'ajoutant à des procédures longues, complexes, coûteuses et chronophages, empêche de nombreuses victimes d'engager un recours. Développer les compétences professionnelles en matière de protection des données chez les avocats et les juges permettrait de rendre disponible cette expertise essentielle et d'accélérer les prises de décisions tout en diminuant la durée des procédures.

Les praticiens du droit déclarent eux-mêmes qu'il existe trop peu de professionnels dans ce domaine et trop peu d'affaires arrivant jusqu'aux tribunaux. Ces commentaires font écho aux difficultés rencontrées par le projet pour trouver des juges et des avocats à interroger dans le cadre de la recherche.

Dans l'ensemble des États membres de l'UE, tout individu peut entamer une procédure judiciaire en recours à des violations de la protection des données. Une fois une telle procédure lancée, il existe un certain nombre de résultats possibles suivant la gravité de la violation et le type de procédure judiciaire initié – civil et administratif, ou pénal.

*« En théorie, un plaignant peut toujours déposer une plainte lui-même, mais ce n'est pas ce que je lui recommanderais de faire. Cela reviendrait à peu de choses près à lui conseiller de s'opérer lui-même le cerveau. » (Avocat, Finlande)*

La recherche empirique sociale souligne deux tendances dans l'ensemble des États membres de l'UE, qui ont des conséquences sur l'efficacité des procédures judiciaires. Très peu de procédures relatives à la protection des données sont engagées. Par conséquent, les juges manquent de compétences et d'expérience dans ce domaine, ce qui donne lieu à une marginalisation des questions de protection des données, qui ne sont pas considérées comme prioritaires lorsqu'il s'agit de programmes de formation et de sensibilisation.

Avis de la FRA

*Les professionnels du droit ont rarement affaire à des cas de protection des données et ne sont par conséquent pas au fait des procédures et des garanties juridiques applicables. Il existe une pénurie de juges spécialisés dans ce domaine.*

*L'UE pourrait soutenir financièrement des activités de formation destinées aux avocats et aux juges portant sur le droit relatif à la protection des données et son application à l'échelle des États membres. Les États membres devraient chercher à renforcer les compétences professionnelles des juges et des avocats dans le domaine de la protection des données en proposant des programmes de formation et en mettant un accent supplémentaire sur les questions de protection des données dans les programmes d'études juridiques. De telles mesures amélioreraient la disponibilité d'une représentation légale suffisamment qualifiée.*

*Renforcer les compétences professionnelles permettrait également de réduire la durée des procédures. Ce manque de compétences est l'un des obstacles qui empêche que des recours soient portés devant les tribunaux, comme le confirment le rapport de la FRA intitulé L'Accès à la justice en Europe : présentation des défis à relever et des opportunités à saisir (2011) ainsi que les résultats de la présente recherche.*

## Conclusions

Il existe de nombreuses manières d'aller de l'avant et d'améliorer la disponibilité et la qualité des voies de recours proposées aux victimes de violations de la protection des données à caractère personnel dans l'UE. L'UE, ses États membres et les autorités de protection des données à caractère personnel ont un rôle à jouer dans le développement de l'approche actuelle relative aux voies de recours mises à leur disposition.

Le rôle des institutions de l'UE est particulièrement important dans ce domaine. La Commission européenne a proposé un projet de règlement qui définit un cadre général de l'UE pour la protection des données à caractère personnel. Le cadre proposé a pour objectif d'harmoniser la législation en matière de protection des données dans l'ensemble des États membres de l'UE et de renforcer la capacité des autorités nationales chargées de la protection des données à engager des recours en cas de violations. Il est essentiel que ces autorités soient indépendantes de tout contrôle extérieur, à la fois en ce qui concerne la distribution et l'allocation de leurs fonds et le recrutement de leur personnel. Une telle indépendance est d'autant plus importante que les autorités de protection des données ont également à traiter des cas de violations commises par l'État. De plus, elles doivent disposer de procédures adéquates, de pouvoirs suffisants et de ressources adaptées, y compris de professionnels qualifiés capables de faire usage de ces pouvoirs et de ces procédures.

L'UE devrait s'efforcer d'augmenter le financement des organisations de la société civile et des organes indépendants capables d'assister les victimes qui engagent des recours dans le domaine de la protection des données à caractère personnel. Afin de renforcer la capacité des victimes à intenter des actions en justice, l'UE devrait envisager un assouplissement des règles régissant la qualité pour agir afin de permettre aux organisations agissant dans

l'intérêt public de déposer des plaintes et ainsi d'ouvrir la voie à des recours collectifs.

Les États membres de l'UE peuvent contribuer à améliorer les mécanismes existants relatifs à la protection des données à caractère personnel en prenant les mesures nécessaires afin de sensibiliser davantage le grand public au sujet de l'existence et du fonctionnement de mécanismes de recours possibles en cas de violations de la protection des données, ainsi que d'organisations de la société civile qui apportent leur soutien aux plaignants. Les États membres devraient également agir en faveur d'un renforcement des compétences professionnelles des juges et des avocats dans le domaine de la protection des données, en proposant des sessions de formation et en mettant davantage l'accent sur les questions de protection des données dans les programmes d'études juridiques. En plus d'assurer la qualité et l'accessibilité d'une représentation juridique, cela permettrait de contribuer à la réduction de la durée des procédures, un point que la recherche sur le terrain a identifié comme constituant un obstacle pour les personnes qui désirent engager un recours.

Les autorités de protection des données à caractère personnel jouent également un rôle crucial en ce qui concerne les droits fondamentaux dans l'UE. Il est essentiel que les personnes qui souhaitent engager un recours leur reconnaissent ce rôle. Ces autorités devraient davantage sensibiliser le grand public en ce qui concerne leur existence et leur action, en cultivant leur image de gardiennes indépendantes des droits fondamentaux dans le domaine de la protection des données. Elles devraient développer une coopération plus étroite avec d'autres gardiens des droits fondamentaux, tels que les organismes chargés des questions d'égalité, les institutions de défense des droits de l'homme et les organisations de la société civile.



Le rapport complet portant sur l'accès aux voies de recours en matière de protection des données à caractère personnel dans les États membres de l'UE (*Access to data protection remedies in EU Member States*), étudie la nature des violations de la protection des données et met en évidence les obstacles rencontrés par les victimes de ces violations lorsqu'elles tentent d'engager un recours. Ce projet socio-juridique de la FRA, qui présente une analyse des régimes de protection des données des 28 États membres de l'UE ainsi que des entretiens menés avec des parties concernées dans 16 États membres, examine les défis auxquels doivent faire face les personnes tentant d'engager de tels recours. Les résultats fournissent des éléments de preuve qui alimenteront les travaux de la Commission européenne et contribueront aux efforts qu'elle déploie en vue de réformer et d'améliorer l'ensemble du régime de protection des données à caractère personnel de l'UE.

## Informations complémentaires :

Le rapport portant sur l'accès aux voies de recours en matière de protection des données à caractère personnel dans les États membres de l'UE (*Access to data protection remedies in EU Member States*) est disponible à : <http://fra.europa.eu/en/publication/2014/access-data-protection-remedies-eu-member-states>

Pour une présentation des activités de la FRA relatives à protection des données, voir : <http://fra.europa.eu/en/theme/data-protection-privacy>

Ce résumé est également disponible en anglais et en allemand et le sera en 2014 également dans les langues suivantes : bulgare, croate, danois, espagnol, estonien, finnois, grec, hongrois, italien, letton, lituanien, néerlandais, polonais, portugais, roumain, slovaque, slovène, suédois et tchèque.



Office des publications

## FRA – AGENCE DES DROITS FONDAMENTAUX DE L'UNION EUROPÉENNE

Schwarzenbergplatz 11 – 1040 Vienne – Autriche  
Tél. +43 158030-0 – Fax: +43 158030-699  
[fra.europa.eu](http://fra.europa.eu) – [info@fra.europa.eu](mailto:info@fra.europa.eu)  
[facebook.com/fundamentalrights](https://www.facebook.com/fundamentalrights)  
[linkedin.com/company/eu-fundamental-rights-agency](https://www.linkedin.com/company/eu-fundamental-rights-agency)  
[twitter.com/EURightsAgency](https://twitter.com/EURightsAgency)



© Agence des droits fondamentaux de l'Union européenne, 2013  
Photo: © SXC

TK-01-13-752-FR-C  
doi:10.2811/5284