# L'étendue dans le temps du droit d'accès aux informations sur les destinataires de données à caractère personnel

De Terwangne , Cécile

*Published in:*
Revue du Droit des Technologies de l'information

*Publication date:*
2011

*Document Version*
le PDF de l'éditeur

# Note d'observations[1]

## L'étendue dans le temps du droit d'accès aux informations sur les destinataires de données à caractère personnel

### INTRODUCTION

La question préjudicielle dont fut saisie la Cour de justice de l'Union européenne dans l'affaire *Rijkeboer*[2] a été l'occasion pour la Cour de clarifier l'étendue dans le temps du droit d'accès à ses données personnelles reconnu à tout individu. Ce droit est établi à l'article 12 de la directive 95/46 relative à la protection des données à caractère personnel[3].

C'est donc à un classique exercice d'interprétation authentique que s'est prêtée la Cour, dans la ligne de l'article 234 CE qui l'invite à interpréter les dispositions du droit communautaire.

La clarification apportée concerne un aspect qui peut à première vue sembler de détail mais qui n'est pas sans importance ni sans conséquences concrètes pour quiconque conserve des données à caractère personnel ou tient un registre contenant de telles données.

C'est un aspect particulier du droit d'accès instauré à l'article 12 qui est en jeu dans cette affaire : l'accès aux informations concernant les destinataires des données à caractère personnel, des données détenues par une administration municipale en l'occurrence. Cette question de l'accès aux données sur les destinataires peut être rapprochée de la question de l'accès aux *log files* ou journaux d'événements. Ces derniers sont en effet des fichiers qui relèvent un certain nombre de renseignements sur toutes les transactions gérées par le serveur. C'est donc à partir de ces journaux et des traces digitales qu'ils conservent que l'on peut identifier les accès qui se sont produits.

L'accès aux données sur les destinataires se heurte directement aux pratiques d'effacement de telles informations au terme d'un certain délai. C'est donc sur le « terrain épineux »[4] de la confrontation entre droit d'accès et limite dans le temps à la conservation des données (sur les communications réalisées) que le renvoi préjudiciel a été formé. En d'autres termes, les juges ont eu à préciser à partir de quand l'exercice du droit d'accès à des informations concernant le passé peut légitimement être paralysé par l'effacement de ces informations. Et pendant combien de temps les personnes détenant des données sont tenues de conserver les traces des actions passées effectuées sur ces données.

La destruction des fichiers de traces (journaux d'événements ou *log files*) entraîne inévitablement pour la personne concernée une perte de contrôle de ses données : « ainsi, la personne qui était en apparence protégée se retrouve lésée, car elle ne connaîtra jamais l'emploi que le possesseur de ses données personnelles a fait de ces dernières »[5].

Pour l'avocat général, cette question de la récupération de la mémoire est délicate. « La

[1] Cécile de Terwangne, professeur à la Faculté de Droit des FUNDP, directrice de recherches au CRIDS.

[2] C.J.C.E., 7 mai 2009, *College van burgemeester en wethouders van Rottredam c. m.e.e. Rijkeboer*, aff. C-553/07.

[3] Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

[4] Conclusions de l'avocat général M. Dámaso Ruiz-Jarabo Colomer présentées le 22 décembre 2008, § 1.

[5] *Ibid.*, § 2.

question de la suppression des traces du passé doit être abordée avec précaution, comme le réclamait Proust en célébrant le pouvoir évocateur du souvenir, car "[l]es lieux que nous avons connus n'appartiennent pas qu'au monde de l'espace où nous les situons pour plus de facilité. Ils n'étaient qu'une mince tranche au milieu d'impressions contiguës qui formaient notre vie d'alors ; le souvenir d'une certaine image n'est que le regret d'un certain instant ; et les maisons, les routes, les avenues sont fugitives, hélas, comme les années"[6] »[7].

La Cour, moins portée sur les évocations littéraires, a pris en considération le fait que la mémoire électronique n'a plus rien de fugitif et que l'effacement est désormais une opération consciente, décidée. L'important est donc de déterminer la durée adéquate de conservation des données en question, en élucidant d'abord cette première question : le droit d'accès vaut-il pour le passé ou le présent ?

## 1. LES FAITS ET LA QUESTION PRÉJUDICIELLE

M. Rijkeboer, citoyen néerlandais, s'est adressé au Collège des bourgmestre et échevins de Rotterdam demandant qu'on l'informe de tous les cas dans lesquels des renseignements sur lui provenant de l'administration communale avaient été communiqués à des tiers. Sa demande couvrait la période des deux années antérieures à sa démarche. Il importait à M. Rijkeboer de connaître l'identité des tiers en question de même que le contenu de l'information transmise. Étant donné qu'il avait déménagé dans une autre commune, il tenait en particulier à découvrir à qui son ancienne adresse avait été communiquée.

Le Collège des bourgmestre et échevins a répondu positivement mais partiellement à cette demande. Il n'a en effet pu donner que l'information correspondant à l'année précédant la demande de M. Rijkeboer. Les données concernant la deuxième année n'étaient plus disponibles car la loi néerlandaise relative aux données personnelles détenues par les administrations communales[8] impose l'effacement des données visées au terme d'un an.

M. Rijkeboer a introduit un recours contre le refus partiel de communication qu'il avait essuyé. Le tribunal de Rotterdam (Rechtbank Rotterdam) estima que la limitation dans le temps de la conservation des informations relatives aux communications de données telle que prévue par la loi n'était pas compatible avec le droit d'être informé consacré à l'article 12 de la directive 95/46. Ce fut alors au tour du Collège d'aller en appel de cette décision devant le Conseil d'État (Raad van State).

Ce dernier, perplexe sur la compatibilité ou non de la disposition de la loi spécifique néerlandaise avec l'article 12 de la directive en question, se tourna vers la Cour de justice afin d'obtenir son interprétation de la portée dans le temps du droit d'être informé contenu dans cet article. Il posa une question préjudicielle que la Cour reformula de la sorte : « question […] visant, en substance, à déterminer si, selon la directive, en particulier son article 12, sous a), le droit d'accès d'une personne à l'information sur les destinataires ou les catégories de destinataires de données à caractère personnel la concernant ainsi que sur le contenu des données communiquées peut être limité à la période d'un an précédant sa demande d'accès »[9].

6 M. Proust, *À la recherche du temps perdu, Du côté de chez Swann*, Gallimard, La Pléiade, Paris 1987, tome I, pp. 419 et 420.

7 Conclusions de l'avocat général, note 4.

8 Wet gemeentelijke basisadministratie persoonsgegevens, Stb. 1994, n° 494.

9 §§ 29 et 31 de l'arrêt.

## 2. LES DISPOSITIONS EN CAUSE DANS LA CONSERVATION ET L'ACCÈS AUX DONNÉES SUR LES DESTINATAIRES

### 2.1. L'article 12 de la directive 95/46 : le droit d'accès

L'article 12 de la directive oblige les États membres à garantir à toute personne concernée le droit d'obtenir du responsable du traitement, « a) sans contrainte, à des intervalles raisonnables et sans délais ou frais excessifs :

– la confirmation que des données la concernant sont ou ne sont pas traitées, ainsi que des informations portant au moins sur les finalités du traitement, les catégories de données sur lesquelles il porte et *les destinataires ou les catégories de destinataires auxquels les données sont communiquées,*
– la communication, sous une forme intelligible, *des données faisant l'objet des traitements*, […] »[10].

Cette disposition confère donc aux individus le droit non seulement de connaître les données les concernant qui font l'objet d'un traitement, mais également certaines informations sur le traitement lui-même. C'est à ce titre que les individus peuvent obtenir le nom des personnes à qui les données sont transmises ou à tout le moins les catégories de tels destinataires. Il s'agit bien, même sur ces points « accessoires » du droit d'accès proprement dit (compris comme l'accès aux données traitées elles-mêmes), d'un véritable droit et non d'une simple possibilité offerte aux personnes concernées.

L'article 12 ne contient aucune précision de délai dans le temps. Il n'est pas indiqué si le droit d'accès sous toutes ses facettes concerne le passé, pas plus que l'éventuelle période du passé qui serait visée[11]. C'est donc à combler ce vide que va s'atteler la Cour (voy. *infra*, points 3 et 4).

### 2.2. L'article 6 de la directive 95/46 : la durée de conservation

La question de l'accès aux *log files* ou aux informations sur les destinataires de données est directement liée à celle du délai de conservation des informations relatives aux opérations effectuées sur les données à caractère personnel conservées, en l'occurrence aux informations relatives aux communications à des tiers. Il est clair que le droit d'accès à l'information sur les destinataires ou les catégories de destinataires des données à caractère personnel ainsi que sur le contenu des données transmises dépend de la durée de conservation de ces données.

Or, la durée de conservation de toute donnée à caractère personnel est visée à l'article 6, § 1er, *littera* e, de la directive. Cette disposition énonce que « […] les données à caractère personnel doivent être […] conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement. […] ».

Ces deux questions entretiennent, selon l'avocat général M. Dámaso Ruiz-Jarabo Colomer[12], une relation de tension. Elles révèlent un conflit interne à la directive entre obligation de suppression des données à caractère personnel dès qu'elles ne présentent plus d'utilité par rapport à la finalité pour laquelle elles ont été enregistrées (article 6 de la directive) et droit d'accès aux informations sur les destinataires des données (article 12 de

10 Nos italiques.

11 Arrêt, § 53.

12 Conclusions de l'avocat général M. Dámaso Ruiz-Jarabo Colomer présentées le 22 décembre 2008.

la directive). Les données relatives aux destinataires étant en effet elles-mêmes des données à caractère personnel, elles ne peuvent être conservées au-delà d'un certain délai. Il est évident qu'« une fois ces données [relatives aux tiers destinataires] effacées conformément à la directive 95/46, la porte au droit d'accès est fermée, puisqu'on ne peut demander une information qui n'existe plus »[13].

Il y a donc un enjeu certain à déterminer le délai adéquat de conservation des données concernant les communications de données, étant donné que cette conservation est cruciale pour permettre l'exercice du droit d'accès.

### 2.3. L'article 16 de la directive : les mesures de sécurité

Même si elle n'est pas entrée dans le champ de réflexion des juges de Luxembourg, il convient d'encore évoquer une troisième disposition liée à la question qui nous occupe.

En fait, on peut relier la question de la conservation des données sur les destinataires et les communications effectuées à l'obligation de prendre des mesures de sécurité adéquates[14]. Les mesures de sécurité doivent en effet notamment garantir les données contre les accès non autorisés. Il est donc essentiel de connaître l'identité des personnes ayant accédé aux données pour vérifier la légitimité de ces accès. On ne pourrait effectuer de vérifications si l'on ne dispose pas de telles informations relatives aux accès réalisés.

C'est précisément cette question qui avait été soumise à la Cour européenne des droits de l'homme dans l'affaire *I. c. Finlande*. Cette affaire concernait une infirmière finlandaise ayant travaillé dans un hôpital dans lequel elle-même, infectée par le virus VIH, était soignée. Soupçonnant ses collègues d'avoir pris subrepticement connaissance de son dossier médical, elle voulut vérifier qui avait accédé à ce dossier. Elle ne put jamais le savoir car son dossier avait dans l'intervalle été archivé, ce qui impliquait l'effacement de toute information concernant les consultations. Au demeurant, le système d'accès prévu par l'hôpital ne conservait les traces que des cinq dernières consultations des dossiers, et l'identification ne se faisait que par service et non par personne effectuant la consultation. Dans son arrêt du 17 juillet 2008[15], la Cour strasbourgeoise a considéré que l'article 8 de la Convention européenne des droits de l'homme impose aux États, au titre de la protection de la vie privée des individus, des obligations positives, notamment en matière de sécurité des données personnelles. Pour la Cour, ce qui est requis c'est une protection réelle et effective des données qui exclut toute possibilité d'accès non autorisé. Un système tel celui qui était pratiqué dans l'hôpital finlandais en question, dans lequel non seulement l'accès aux dossiers médicaux n'est pas restreint aux professionnels de la santé directement impliqués dans le traitement du patient, mais en outre il n'est pas tenu de registre de toutes les personnes qui ont eu accès au dossier, est insatisfaisant et en violation avec l'article 8 de la CEDH.

Les obligations d'entourer les données personnelles de mesures de protection vont donc de pair avec la possibilité pour les personnes concernées d'effectuer un contrôle rétrospectif des accès à leurs données.

13 Conclusions de l'avocat général, § 16.

14 Article 17 de la directive : « Sécurité des traitements. 1. Les États membres prévoient que le responsable du traitement doit mettre en œuvre les mesures techniques et d'organisation appropriées pour *protéger les données à caractère personnel contre* la destruction accidentelle ou illicite, la perte accidentelle, l'altération, *la diffusion ou l'accès non autorisés*, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite » (nos italiques).

15 Cour eur. D.H., *I. c. Finlande*, arrêt du 17 juillet 2008, req. n° 20511/03.

## 3. INTERPRÉTATION DE L'ARTICLE 12 : VAUT-IL POUR LE PRÉSENT OU POUR LE PASSÉ ?

### 3.1. Le droit d'accès aux données sur les destinataires ne vaut-il que pour le présent ?

Le Collège des bourgmestre et échevins de Rotterdam de même que les plaideurs des Pays-Bas, de la République tchèque, de l'Espagne et du Royaume-Uni ont soutenu « que le droit d'accès à l'information sur les destinataires ou les catégories de destinataires visé à l'article 12, sous a), de la directive n'existe que pour le présent et non pour le passé. Dès lors que les données ont été effacées, conformément à la réglementation nationale, la personne concernée ne peut plus y avoir accès »[16].

Pour le Collège et le gouvernement des Pays-Bas, le régime mis en place par la loi spécifique néerlandaise qui permet aux communes d'informer tout administré, à sa demande, des données communiquées à des destinataires au cours de l'année précédente, va d'ailleurs au-delà des exigences imposées par la directive[17].

Si on peut comprendre le souci de ces États intervenus à la cause de limiter les implications pratiques de la législation de protection des données, en l'occurrence le poids de la conservation des traces des actions effectuées sur les données, on ne peut qu'être interpellé par ce que cela signifie pour le droit d'accès. Ainsi, la capacité de connaître les destinataires de ses données ne vaudrait qu'à partir du moment où on formule une demande au responsable du traitement ? Ce ne sont donc que les destinataires envisagés à ce moment-là qui doivent être révélés ? Quelle chimère de droit d'accès qu'un droit qui ne vaut que pour aujourd'hui et demain et ne permet aucun contrôle sur hier…

Dans une série de cas, c'est précisément parce que l'on s'est rendu compte de quelque chose de douteux ou parce que l'on souhaite savoir à quelle source des personnes ont obtenu des informations, que l'on exerce son droit d'accès pour découvrir les personnes à qui les données ont été transmises. À suivre le raisonnement de ces gouvernements, si l'on veut vérifier un certain temps après avoir reçu les informations sur les catégories de destinataires des données quelles ont été réellement les personnes à qui on a transmis les données, on ne pourra pas les connaître et donc pas s'assurer du respect de ce qui a été annoncé.

### 3.2. Le droit d'accès aux données sur les destinataires vaut aussi pour le passé

Or, si la protection des données est réalisée par la mise en place d'un ensemble d'exigences concernant le traitement des données, elle l'est également par l'octroi de droits permettant aux individus sur qui portent les données de contrôler le sort réservé à leurs données. Le droit d'accès, riche de toutes ses facettes, a pour vocation « que la personne concernée puisse s'assurer que ses données à caractère personnel sont traitées de manière exacte et licite, c'est-à-dire, en particulier, que les données de base la concernant sont exactes et qu'elles sont adressées à des destinataires autorisés »[18]. Le quarante et unième considérant de la directive expose expressément la finalité du droit d'accès qui est la possibilité d'effectuer des vérifications de l'usage des données traitées.

Outre ce but de permettre le contrôle, le droit d'accès est la condition de l'exercice des autres droits garantis par la directive.

Ainsi, c'est à la suite de l'obtention d'informations par le biais de la mise en œuvre du droit d'accès que la personne concernée sera en

[16] § 37 de l'arrêt.

[17] § 38 de l'arrêt.

[18] § 49 de l'arrêt.

mesure de se rendre compte d'erreurs, omissions, incomplétudes ou non mises à jour de ses données. Ce n'est qu'alors qu'elle pourra envisager d'exercer son droit de correction[19] afin de faire effectuer la rectification, l'effacement ou le verrouillage des données qui s'imposent[20].

De la même manière, le droit d'accès permet l'exercice du droit d'opposition prévu à l'article 14 de la directive. Et c'est encore lui la plupart du temps qui est à la base de la découverte de traitements ou d'opérations illicites sur ses données qui donne à la personne concernée la possibilité d'exercer son droit de recours afin d'obtenir réparation du dommage encouru[21] [22].

« Il convient de constater que, pour assurer l'effet utile des dispositions visées aux points 51 et 52 du présent arrêt, ce droit doit nécessairement concerner le passé », a observé la Cour[23]. Nul ne serait en mesure de mettre en œuvre de manière efficace ses droits de correction et d'opposition ni son droit à réparation du préjudice subi s'il ne peut disposer des données du passé.

Il est d'ailleurs à noter que le droit de correction instauré par la directive s'accompagne d'un droit de suite, c'est-à-dire le droit de voir informer de la correction à apporter aux données les personnes à qui ces données ont été antérieurement transmises. En d'autres termes, le responsable du fichier a l'obligation de faire suivre les rectifications, effacement ou verrouillage auxquels il a dû procéder « aux tiers auxquels les données *ont été communiquées* »[24]. La forme passée du verbe repris dans la disposition de la directive indique bien qu'il s'agit des destinataires à qui les données ont été transmises *antérieurement* à la correction apportée.

Le responsable du traitement est dispensé de cette obligation si l'honorer s'avère impossible ou implique des efforts disproportionnés. Cette précision de l'article 12, *littera* c, servira à la Cour, ainsi qu'on le verra au point suivant, pour déterminer la période du passé visée par l'obligation de conserver des traces pour permettre l'exercice utile du droit d'accès et, à travers lui, des autres droits consacrés dans la directive.

La Cour de justice a répondu à la première partie de la question soulevée par le Raad van State néerlandais : « L'article 12, sous a), de la directive impose aux États membres de prévoir un droit d'accès à l'information sur les destinataires ou les catégories de destinataires des données ainsi qu'au contenu de l'information communiquée non seulement pour le présent, mais aussi pour le passé »[25].

## 4. DÉTERMINATION DU DÉLAI DE CONSERVATION

Une fois admis, à l'instar de la Commission européenne et de la Grèce également intervenue à la cause, que la directive prévoit un droit d'accès non seulement pour le présent mais aussi pour la période antérieure à la demande d'accès, il restait à la Cour à préciser l'étendue du droit d'accès dans le passé. Il semble en effet évident pour tous qu'il ne s'agit

19 Prévu à l'article 12, *littera* b de la directive 95/46.

20 § 51 de l'arrêt.

21 L'article 22 de la directive impose aux États membres de mettre à disposition des personnes lésées un droit de recours juridictionnel en cas de violation des droits garantis par la législation de protection des données. L'article 23, § 1er dispose : « Les États membres prévoient que toute personne ayant subi un dommage du fait d'un traitement illicite ou de toute action incompatible avec les dispositions nationales prises en application de la présente directive a le droit d'obtenir du responsable du traitement réparation du préjudice subi ».

22 § 52 de l'arrêt.

23 § 54 de l'arrêt.

24 Article 12, *littera* c de la directive 95/46. Nos italiques.

25 § 70 de l'arrêt.

pas d'imposer le maintien dans le temps sans limite des journaux de connexions ou traces des communications de données.

La Cour reconnaît d'emblée que les États membres disposent d'une certaine marge de manœuvre pour transposer l'article 12 et, en l'occurrence, établir le délai de conservation des traces des communications, mais elle signale dans le même temps que cette marge n'est pas illimitée[26]. Elle s'emploie donc à indiquer les balises pour cet établissement.

La Cour raisonne à partir de la finalité de l'établissement d'une période de conservation des données, finalité déterminante pour l'exercice. « L'établissement d'un délai relatif au droit d'accès à l'information sur les destinataires ou les catégories de destinataires et le contenu des données communiquées doit permettre à la personne concernée d'exercer les différents droits prévus par la directive et rappelés aux points 51 et 52 du présent arrêt »[27]. Il s'agit bien d'établir un délai qui donne effet utile aux divers droits de la personne concernée.

Par la suite, la Haute juridiction relève divers paramètres qui peuvent influer sur la détermination du délai de conservation obligatoire.

### 4.1. Les paramètres intervenant dans l'établissement du délai de conservation

Plusieurs paramètres sont à prendre en considération par les États membres, plus ou moins déterminants[28].

Tout d'abord, la durée de conservation des données à caractère personnel « de base » ou « principales », celles qui font l'objet du traitement et dont les données relatives aux destinataires et aux communications peuvent être considérées comme « accessoires ». En présence de cas où ces données principales font elles-mêmes l'objet d'une très longue durée de conservation, l'intérêt d'exercer les droits et d'intenter les recours prévus peut s'estomper au fil du temps pour les personnes concernées. On peut donc vraisemblablement s'épargner le poids d'une conservation qui remonte trop loin dans le temps. Cela étant, l'intervention du critère de proportionnalité dont il est question au point suivant s'oppose à une durée de conservation des traces des communications qui ne serait pas dans un juste rapport de proportionnalité avec la durée de conservation des données principales.

Au titre des paramètres à retenir figurent également assez logiquement les délais existants pour introduire un recours.

La Cour suggère aussi de tenir compte de la nature plus ou moins sensible des données principales. Les données sensibles étant par nature davantage susceptibles que les autres de générer un dommage pour la personne concernée ou d'être source de discrimination lorsqu'elles font l'objet d'un traitement, la Cour estime sans doute qu'il faut permettre un contrôle accru de la part des personnes concernées. Afin de leur permettre d'exercer leurs droits, il faut donc garantir une plus grande disponibilité des données accessoires, notamment des journaux de connexions, nécessaires pour effectuer les vérifications et surveillances.

Enfin, la Cour propose encore comme paramètres le nombre des destinataires concernés et la fréquence des communications.

### 4.2. L'intervention du critère de proportionnalité

Un dernier élément est appelé à intervenir dans la détermination du délai de conservation des données relatives aux destinataires et au contenu des communications. Il s'agit du critère de proportionnalité.

[26] § 56 de l'arrêt.

[27] § 57 de l'arrêt.

[28] Voy. les §§ 58-59 et 63 de l'arrêt.

C'est en raisonnant par analogie que la Cour a conclu à l'intervention de ce critère[29]. Elle a en effet observé que, à plus d'une reprise, la directive veille à ne pas faire peser sur les responsables de traitement des obligations disproportionnées, des charges excessives. Ainsi, le devoir de faire suivre aux tiers les corrections apportées aux données ne vaut plus si cette démarche s'avère impossible ou suppose des efforts disproportionnés (article 12, *littera* c, *in fine*). Il en est de même pour le devoir d'information (article 11, § 2). Et l'obligation de prévoir des mesures de sécurité pour encadrer le traitement des données s'entend comme l'obligation de prendre les mesures appropriées au regard des risques, en tenant compte des coûts que cela représente pour le responsable (article 17).

On peut donc transposer ce souci à la question de la durée de conservation des données « accessoires ». Les États ne doivent pas fixer un délai de conservation qui conduise à une charge excessive pour le responsable du traitement tenu de veiller à la conservation.

La Cour a indiqué[30] qu'une réglementation limitant la durée de conservation à un an alors que les données principales sont, elles, conservées pour une très longue durée (il s'agissait en l'espèce de données contenues dans les registres tenus par la commune) ne peut être admise comme instaurant un juste équilibre entre les intérêts et obligation en présence. Ce n'est que s'il est prouvé qu'une conservation plus longue constituerait une charge excessive pour le responsable du traitement que l'on pourrait estimer la réglementation conforme avec la directive.

## CONCLUSION

L'affaire *Rijkeboer* aura été l'occasion pour la Cour de justice de clarifier l'étendue dans le temps du droit d'accès instauré par la directive. C'est particulièrement une facette du droit d'accès qui a retenu l'attention de la Cour : le droit d'être informé des destinataires ou à tout le moins des catégories de destinataires à qui les données sont communiquées ainsi que du contenu des communications. Le sens même d'un tel droit étant de permettre aux individus concernés par des données traitées de prendre connaissance du sort réservé à leurs données et de procéder à des vérifications des opérations effectuées sur elles, afin d'être à même d'exercer leurs autres droits prévus par la directive, il est impératif que l'accès ne soit pas réduit au présent mais couvre également le passé.

Il ne s'agit pas pour autant de permettre de remonter sans limite dans le temps, ce qui induirait une obligation corrélative pour les responsables de conserver indéfiniment les données relatives aux actions réalisées avec les données de base, en l'occurrence aux communications de ces données. La fixation d'un délai de conservation légitime varie en fonction de paramètres et doit être tempérée par l'intervention du critère de proportionnalité.

La Cour a donc conclu que les États membres sont tenus de fixer un délai de conservation de l'information sur les destinataires ou les catégories de destinataires et le contenu des données communiquées et de prévoir un accès à cette information qui constituent un juste équilibre entre, d'une part, l'intérêt de la personne concernée à protéger sa vie privée, notamment au moyen des voies d'intervention en cas de non-conformité du traitement de ses données avec la directive, ainsi que des droits d'opposition et d'introduction d'un recours juridictionnel et, d'autre part, la charge

[29] « Des considérations analogues sont pertinentes s'agissant de l'établissement d'un délai relatif au droit d'accès à l'information sur les destinataires ou les catégories de destinataires ainsi que sur le contenu des données communiquées » (§ 63 de l'arrêt).

[30] § 66 de l'arrêt.

que l'obligation de conserver cette information représente pour le responsable du traitement[31].

L'arrêt *Rijkeboer* présente un enseignement concret pour les responsables de traitement. Ils savent à l'avenir que découle de la directive (et dès lors des lois nationales qui l'ont transposée) l'obligation de veiller à la conservation des traces des communications et des accès aux données accordés à des tiers pendant à tout le moins une durée raisonnable, afin de permettre aux personnes concernées d'être informées, à leur demande, de ces transmissions de leurs données et de pouvoir en contrôler la licéité.

La difficulté réside en ce que la Cour invite les législateurs nationaux à faire l'exercice de fixer des délais de conservation. Or, ces délais sont très variables et dépendent des circonstances propres à chaque situation. Si certaines catégories de traitements de données pourront être traitées de façon collective et se voir indiquer un délai uniforme de conservation des données relatives aux communications aux tiers, bon nombre d'autres traitements ne pourront entrer dans des catégories prédéfinies. Cela semble plus évident pour les cas de traitements au sein du secteur public comme dans l'affaire confiée à la Cour, mais on imagine difficilement les législateurs nationaux détailler pour tous les types de traitements de données envisageables (autant dire une myriade) la durée idoine de conservation des données relatives aux communications. Les responsables, sur le terrain, seront donc laissés à une incertitude quant à la validité de la durée qu'ils auront déterminée eux-mêmes sur la base des critères proposés par la Cour.

Cet enseignement s'inscrit dans la même ligne que celui qui se dégage de l'arrêt *I c. Finlande* prononcé par la Cour européenne des droits de l'homme[32]. Sans avoir à se prononcer sur la durée de conservation des données relatives aux accès, la juridiction strasbourgeoise a estimé qu'un système qui n'individualise pas les traces des accès aux données ni ne conserve durablement ces traces et ne permet donc pas à la personne concernée de vérifier rétrospectivement la légalité de ces accès, n'est pas conforme aux exigences découlant de l'article 8 de la CEDH.

Cécile de Terwangne

[31] §§ 64 et 70 de l'arrêt.

[32] Voy. *supra*.