Chronique du droit « Post-Snowden » : La CJUE et la CEDH sonnent le glas de la surveillance de masse

Protection des données personnelles (CEDH et CDFUE)

Jean-Philippe Foegle

Édition électronique

URL : <http://journals.openedition.org/revdh/2074>

DOI : 10.4000/revdh.2074

ISSN : 2264-119X

Éditeur

Centre de recherches et d'études sur les droits fondamentaux

Référence électronique

Jean-Philippe Foegle, « Chronique du droit « Post-Snowden » : La CJUE et la CEDH sonnent le glas de la surveillance de masse », *La Revue des droits de l'homme* [En ligne], Actualités Droits-Libertés, mis en ligne le 30 mars 2016, consulté le 19 avril 2019. URL : <http://journals.openedition.org/revdh/2074> ; DOI : 10.4000/revdh.2074

Ce document a été généré automatiquement le 19 avril 2019.

Tous droits réservés

Chronique du droit « Post-Snowden » : La CJUE et la CEDH sonnent le glas de la surveillance de masse

Protection des données personnelles (CEDH et CDFUE)

Jean-Philippe Foegle

- 1 « Pour la première fois depuis le 11 septembre, nous discernons les contours d'une politique qui tourne le dos à la réaction et à la peur pour embrasser la résilience et la raison »¹. Tandis que le maintien et la constitutionnalisation d'un état d'exception destiné à lutter contre le terrorisme laisse à voir un mouvement presque inexorable d'inversion des hiérarchies traditionnelles entre sécurités et libertés², les propos suscités d'Edward Snowden apparaissent inscrits à contre-courant du mouvement dominant. Inédites par leur ampleur et leur retentissement tant médiatique que géopolitique, les révélations de ce lanceur d'alerte³ trouvent en effet un écho sans cesse renouvelé dans l'espace public, suscitant nombre de « contre-feux » face à la surveillance de masse. En Europe, après la retentissante décision *Digital Rights Ireland* de 2014⁴, nombre de juridictions nationales ont – à l'inverse du Conseil Constitutionnel – pris leurs responsabilités et procédé à une invalidation des lois sur la surveillance électronique sur le fondement de la Charte des Droits Fondamentaux, notamment au Royaume-Uni⁵. Aux Etats-Unis, l'invalidation de l'article 215 de la FISA pour des motifs purement techniques avait préparé la réforme en demi-teinte du Patriot Act par le Freedom Act⁶ qui, sous couvert de favoriser les libertés, conforte en réalité l'arsenal de surveillance dont disposent les agences nord-américaines de renseignement⁷.
- 2 Les arrêts commentés poursuivent et amplifient ce mouvement. D'une part, le 6 octobre 2015, la Cour de Justice de l'Union Européenne a invalidé la décision 2000/520/CE relative aux transferts de données à caractère personnel vers les États-Unis validant les principes dits de la « Sphère de sécurité » ou Safe Harbor qui constituaient auparavant le fondement des transferts de données de l'Union Européenne vers les Etats-Unis. Dans un contexte d'interactions croissantes entre le droit de la Convention Européenne des droits de l'Homme et de concurrences en matière de protection des droits fondamentaux⁸, il est

remarquable de noter que la Cour de Strasbourg a, elle aussi, opéré une condamnation stricte de la surveillance de masse dans son arrêt Zakharov⁹ puis dans son arrêt Szabo¹⁰, ce qui ne manquera pas d'avoir une incidence sur les recours pendants devant les juges de Strasbourg – et notamment le recours contre la législation anglaise en matière de recueil des données de connexion¹¹.

- 3 Or, prises dans leur ensemble et bien que l'arrêt Sakharov ait un impact immédiat moins fort que l'arrêt Schrems, ces arrêts témoignent d'une montée en généralité radicale de l'argumentation en matière de protection de la vie privée, qui marque cette fois ci, par un curieux jeu d'allers-retours entre droit américain et droit de l'Union, l'apparition plus nette d'un paradigme constitutionnel en matière de protection des données personnelles¹², marqué par une ouverture des prétoires aux citoyens et un renforcement significatif de leurs garanties procédurales d'une part, et par une condamnation – ambiguë (comme nous le verrons en conclusion) – du principe même de la surveillance de masse d'autre part.
- 4 Mais venons-en aux faits de l'espèce. Si les faits de l'arrêt Zakharov, qui concernait le recours d'un membre de l'opposition russe suspectant une mise sous surveillance de ses communications, ne présente pas de spécificité particulière, le contentieux du « Safe Harbor » est en revanche plus complexe à aborder et mérite que l'on revienne sur son contexte. Aux origines des questions de droit posées dans l'affaire Schrems, il y a en effet la décision 2000/520/CE relative aux transferts de données personnelles vers les Etats-Unis, plus couramment nommé la « Décision Safe Harbor » ou, en Français, « décision sur la sphère de sécurité », prise sur le fondement de la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995. L'article 25, paragraphe 1 de cette directive pose en effet un principe selon lequel le transfert vers un pays tiers de données à caractère personnel faisant l'objet d'un traitement ne peut avoir lieu que si le pays tiers en question assure un niveau de protection « adéquat » à de telles données¹³, ce qui peut être constaté par une décision de la Commission. Inversement, le considérant 57 de la même directive prévoit la possibilité d'interdire un transfert de données à caractère personnel vers un pays-tiers lorsque celui-ci n'offre pas ledit niveau de protection.
- 5 Certes, de nombreuses exceptions sont prévues à l'article 26 de la directive, qui permet notamment le transfert des données vers un pays n'assurant pas une protection de ce type dès lors que « la personne concernée [a] indubitablement donné son consentement au transfert envisagé », ou par le biais de clauses contractuelles adéquates, encadrées par la directive et une décision de la Commission¹⁴ et qui doivent être insérées par les entreprises dans les contrats signés avec des personnes situées en Europe. Ces solutions sont néanmoins plus complexes à mettre en œuvre et plus contraignantes pour les acteurs économiques, de sorte qu'elles apparaissent moins pertinentes au regard de l'objectif de la directive de 1995 de favoriser la libre-circulation des flux de données. C'est précisément pour assurer la fluidité des flux transatlantiques de données malgré d'importantes divergences d'approche de la protection de la vie privée¹⁵ que la commission a validé, par sa décision de 2000, les « Principes de la sphère de sécurité » ainsi que la « Foire aux Questions » publiée par le département américain du commerce, considérant que ceux-ci offraient une protection « adéquate » aux citoyens européens dont les données sont transférées vers les Etats-Unis.
- 6 Cette décision, issue d'après négociations entre la Commission et les négociateurs américains¹⁶, avait été prise à la suite d'une série d'avis du G29¹⁷ et du comité de l'article 31, et faisait reposer la protection des données personnelles des citoyens de l'Union sur

un système fort complexe d'auto-certification des acteurs économiques, obligeant les entreprises adhérentes nord-américaines à respecter une série de principes pour pouvoir bénéficier de la présomption de « niveau de protection adéquat » que prévoit celle-ci et, ainsi, pouvoir traiter en toute légalité les données des européens. Ceux-ci prévoyaient notamment une obligation d'informer les personnes sur les raisons de la collecte de leurs données, sur les usages ultérieurs de celles-ci et les moyens de limiter l'utilisation et la divulgation de celles-ci, mais également de ménager un droit de recours aux personnes concernées par le non-respect des principes, et de sanctionner le cas échéant les organisations responsables de ce non-respect¹⁸. Un ensemble complexe de mécanismes hybrides mêlant arbitrage privé et contrôle par les pouvoirs publics, existaient pour vérifier le respect des principes de la sphère de sécurité. Dans ce cadre, la Federal Trade Commission et le ministère du Transport des Etats-Unis pouvaient en dernier recours prendre des mesures sur la base des pouvoirs qui leur étaient conférés, notamment ceux de diligenter des enquêtes et de prononcer le cas échéant des sanctions à l'encontre des entreprises récalcitrantes¹⁹.

- 7 Enfin et il s'agit d'un aspect essentiel de ce système au regard du présent litige, le quatrième alinéa de l'annexe I de la décision 2000/520, disposait que les obligations imposées par les principes de la sphère de sécurité peuvent ne pas être appliquées par les organisations, lorsque cela est justifié par « les exigences relatives à la sécurité nationale, l'intérêt public et le respect des lois des États-Unis » et par « les textes législatifs, les règlements administratifs ou les décisions jurisprudentielles qui créent des obligations contradictoires ou prévoient des autorisations explicites », à condition que les organisations puissent alors démontrer que le non-respect des principes est limité « aux mesures nécessaires pour garantir les intérêts légitimes que cette autorisation vise à servir ». En clair, les organisations adhérentes au Safe Harbor avaient l'obligation de coopérer avec les agences de renseignement pour détecter les atteintes potentielles à la sécurité nationale, et cette obligation primait sur le respect du droit à la protection des données personnelles des Européens.
- 8 Par la suite, le régime ainsi mis en place avait fait l'objet de deux évaluations de la part de la Commission européenne en 2002²⁰ et 2004²¹, ainsi que d'une évaluation indépendante de 2008²² qui avaient mis en lumière les insuffisances de la sphère de sécurité, et notamment son caractère peu contraignant et, partant, peu effectif. Étaient notamment en cause les dérives du système d'auto-certification et la faiblesse du contrôle opéré par la Federal Trade Commission du non-respect des principes du Safe Harbour, conduisant de nombreuses entreprises à effectuer de fausses déclarations d'adhésion au « Safe Harbour » en toute impunité²³. Les critiques se firent effet plus acerbes après la révélation par de l'ampleur des atteintes possibles à la vie privée des citoyens de l'Union autorisée par le « Patriot Act » de 2001, une étude de chercheurs indépendants ayant conclu à l'incompatibilité radicale de la protection européenne des données personnelles avec l'arsenal de surveillance prévu par ce texte²⁴. Surtout, et il s'agit d'une considération d'opportunité qui n'est pas sans lien avec la présente décision, la Commission Européenne avait elle-même procédé à une critique en règle de cette décision²⁵ tout en se contentant d'annoncer qu'elle entendait « entamer de toute urgence un dialogue avec les autorités américaines afin d'examiner les lacunes mises en évidence » remettant aux calendres grecques la protection effective de la vie privée des personnes.
- 9 Ironie du sort ou remake de David contre Goliath, c'est finalement la pugnacité d'un étudiant en droit, Maximilian Schrems qui a porté le coup de grâce à cet accord par

ailleurs fortement contesté depuis 2013, y compris par la Commission européenne elle-même. Interpellé par les révélations d'Edward Snowden sur le programme PRISM et sur la collaboration désormais établie des « géants » du numérique et notamment le réseau social Facebook, celui-ci décide de saisir le commissaire Irlandais à la protection des données personnelles d'une plainte visant à faire interdire le transfert de ses données vers les Etats-Unis par Facebook Ireland.

- 10 Le commissaire ayant rejeté la plainte en cause, M. Schrems saisit par la suite la High Court Irlandaise d'une demande tendant, en substance à forcer le commissaire à faire usage de ses pouvoirs et à procéder à l'interdiction du transfert de ses données par Facebook Ireland vers les Etats-Unis²⁶. Cela visait, en réalité, à faire invalider le régime juridique de la « sphère de sécurité » sur le fondement de la directive 1995/46/CE d'une part, et des articles 7 et 8 de la Charte des Droits Fondamentaux de l'Union Européenne d'autre part²⁷. Plus précisément encore, M. Schrems, se fondant sur les révélations à propos du programme « Prism », considérait que les données personnelles des internautes n'étaient pas protégées contre les intrusions dues à la surveillance étatique, notamment en raison du fait que les agences de renseignement nord-américaines pouvaient avoir un accès illimité aux données transférées sans qu'il soit nécessaire d'obtenir une décision juridictionnelle en ce sens, ce qui serait contraire aux protections instaurées par la directive 1995/CE et par l'article 7 de la Charte des Droits Fondamentaux de l'Union Européenne protégeant les données personnelles. Confrontée à une question de droit inédite ou presque, la High Court Irlandaise, saisie du refus du Commissaire a décidé de surseoir à statuer, renvoyant à la Cour de Justice de l'Union Européenne une question préjudicielle, non sans avoir procédé à une critique acerbe des programmes mis en place par la National Security Agency qu'elle n'hésita pas à comparer à la surveillance exercée par la Stasi sur les ressortissants de l'Allemagne de l'Est²⁸. Une décision sur ce point était d'autant plus attendue que le retentissant arrêt « Digital Rights Ireland » de 2014 avait invalidé un système particulièrement intrusif de collecte des métadonnées des internautes européens tout en laissant nombre de questions en suspens²⁹.
- 11 Par une décision dépourvue cette fois-ci d'ambiguïtés, la Grande Chambre de la CJUE a jugé, d'une part, que l'existence d'une décision de la Commission constatant le caractère « adéquat » de la protection des données dans un pays tiers ne fait pas obstacle à ce qu'une autorité de contrôle d'un État membre examine la demande d'une personne relative à la protection de ses droits et libertés à l'égard du traitement de données à caractère personnel la concernant. D'autre part surtout, la Cour de justice a invalidé la décision Safe Harbor en ce que celle-ci, permettant aux autorités publiques nord-américaines d'accéder de manière généralisée au contenu de communications électroniques hors de tout contrôle effectif d'une autorité indépendante, et n'assure pas une protection adéquate des données personnelles.
- 12 Ce faisant, la CJUE consacre une exigence de triple continuité de la protection des données des données personnelles (1°). Surtout, la Cour valide implicitement les critiques formulées à l'égard d'un système marqué par sa complexité, et dont le caractère attentatoire aux droits fondamentaux a été mis en lumière par les révélations Snowden. Si l'on fait l'effort d'analyser la décision en la mettant en lien avec les arrêts Zakharov et Szabo, force est alors de constater principe même de la surveillance « de masse » est ainsi sévèrement condamné en droit européen des droits de l'Homme, si bien que sa survie apparaît plus que jamais illusoire. Mais, nous le constaterons in fine, une telle position n'est pas dépourvue d'ambiguïtés (2°).

1°/- L'exigence renforcée d'une triple continuité de la protection des données personnelles des citoyens européens

- 13 Par son arrêt Schrems, la Cour consacre une triple continuité de la protection des citoyens de l'Union. Continuité du contrôle des usages des données d'une part, car le contrôle opéré par la Commission européenne sur l'existence d'un niveau de protection « adéquat » de la vie privée dans un pays-tiers n'annihile pas celui qui peut être opéré par les autorités nationales de contrôle. Continuité géographique de cette protection ensuite, car la Cour exige que le niveau de protection des données personnelles transférées vers un pays-tiers soit substantiellement équivalent à la protection accordée aux données traitées sur le territoire de l'UE. Continuité temporelle enfin, car la Cour exige que les régimes juridiques encadrant les transferts de donnée fassent l'objet d'une révision régulière de leur compatibilité aux droits fondamentaux consacrés par l'UE.

A - Une continuité des contrôles exercés sur les usages des données

- 14 Avant de parvenir à cette consécration, la Cour faisait toutefois face à une contrainte juridique de taille, à savoir celle de concilier tout à la fois l'autorité des décisions des instances de l'Union d'une part, et l'exigence de maintenir un niveau élevé de garantie des droits fondamentaux des citoyens de l'Union d'autre part. En effet, comme l'avait souligné le commissaire irlandais à la protection des données personnelles³⁰, les États membres et leurs organes ont l'obligation de faire application d'une décision de la Commission reconnaissant l'existence d'une garantie « adéquate » de protection des droits fondamentaux dans l'ordre juridique nord-américain, car les actes des institutions de l'Union jouissent, en principe, d'une présomption de légalité³¹ en raison de l'article 288-3 du TFUE. Dans ce cadre, la Cour était confrontée à un dilemme peu soluble, à savoir celui d'assurer l'unité du droit européen au risque de violations des droits fondamentaux, ou d'assurer la protection des droits fondamentaux au risque d'une balkanisation du droit de l'Union³². Une vision étroitement techniciste de l'autorité des décisions des institutions de l'Union européenne aurait dû conduire la Cour à rejeter la demande de Max Schrems et à valider le raisonnement du commissaire à la protection des données personnelles irlandais, qui s'était estimé lié par la décision de la Commission³³. Or, un tel rejet aurait conduit à limiter drastiquement les possibilités de mise en cause du Safe Harbour par les citoyens européens et à conférer à celui-ci un brevet de conformité au droit primaire. Et ce, d'autant plus que la décision elle-même ne prévoyait la possibilité de suspendre les transferts de données que dans des hypothèses très restrictivement définies.
- 15 Refusant d'être enfermée dans une alternative binaire, la Cour se place d'emblée sur le terrain du droit primaire et de la Charte des Droits Fondamentaux, légitimant par la même occasion l'atteinte supposément portée à l'autorité du droit tout en aménageant ses effets. Ce sont en effet, comme dans l'arrêt « Google Spain »³⁴ et au prix d'une montée en généralité significative de l'argumentation de la Cour, des considérations de pleine effectivité des droits fondamentaux consacrés par la Charte des Droits Fondamentaux qui

conduisent la Cour à se fonder sur son article 8§3 pour consacrer une exigence d'accès effectif et continu des citoyens à un contrôle indépendant des usages de leurs données. Rappelant ainsi d'emblée que les dispositions de la directive 95/46, doivent nécessairement, selon une jurisprudence constante, être interprétées à la lumière des droits fondamentaux garantis par la Charte³⁵; et de l'objectif de garantir une protection efficace et complète des libertés et des droits fondamentaux des personnes physiques³⁶ (arrêt Schrems, §39), les juges procèdent à une lecture constructive du rôle des autorités nationales de contrôle, et ce par un raisonnement en trois temps.

- 16 En tout premier lieu, la Cour rappelle sans surprise – mais non sans un certain lyrisme juridictionnel – que l'institution d'autorités indépendantes dans les Etats membres résulte, selon une jurisprudence constante, d'une double exigence issue de l'article 8, paragraphe 3, de la CDFUE et de l'article 16, paragraphe 2, TFUE et constitue à ce titre un élément essentiel du respect de la protection des personnes à l'égard du traitement des données à caractère personnel³⁷ (arrêt Schrems, §41). Or, le délicat exercice de conciliation entre le respect du droit fondamental à la vie privée et les intérêts économiques liés à la libre circulation des données à caractère personnel³⁸ que doivent opérer ces instances implique que celles-ci puissent disposer d'un large éventail de pouvoirs dont, notamment, des pouvoirs d'investigation, et des pouvoirs effectifs de sanction et d'intervention tels que celui d'interdire temporairement ou définitivement un traitement de données ou encore – et surtout – celui d'ester en justice (arrêt Schrems, §42 et 43).
- 17 Le rappel du fondement « constitutionnel » des pouvoirs dont disposent les autorités nationales n'est en rien anodin : il s'agit ici, dans la continuité des méthodes « téléologiques » d'interprétation du juge de l'Union inaugurées par l'arrêt Van Gend en Loos³⁹ de contourner une contrainte juridique liée à l'architecture générale de la directive de 1995. Celle-ci a en effet créé deux régimes différents de protection des citoyens de l'Union : un régime général prévu au chapitre II de celle-ci – qui encadre les traitements de données personnelles effectués sur le territoire de l'Union – et un régime spécifique aux transferts de données vers les pays-tiers prévu au chapitre IV. Or précisément, les juges de Luxembourg avaient énoncé dans l'arrêt Lindqvist que ce chapitre a mis en place un régime « complémentaire au régime général »⁴⁰ insistant spécifiquement dans la suite de l'arrêt sur la spécificité de ce régime, qui ne doit pas être conçu comme une « copie conforme » du régime général. On le comprend aisément dans la mesure où les transferts de données vers des pays-tiers doivent tenir compte des spécificités des systèmes juridiques étrangers et éviter des hypothèses de conflit qui avaient marqué le début des négociations sur le Safe harbour⁴¹. Cet arrêt avait longtemps été lu – non sans raisons – par la doctrine comme impliquant que les citoyens ne peuvent disposer du même niveau de garanties lorsque leurs données sont transférées vers un pays-tiers⁴², et ce d'autant plus que le caractère « adéquat » de la protection qui doit être accordée ne signifie pas que cette même protection doive être identique à celle accordée sur le territoire des pays membres de l'Union européenne.
- 18 C'est à une toute autre lecture de l'arrêt Linqvist à laquelle s'est toutefois livrée la Cour. Ayant énoncé sans surprise que l'opération consistant à faire transférer des données à caractère personnel depuis un Etat membre vers un pays tiers « constitue, en tant que telle, un traitement de données à caractère personnel au sens de l'article 2, sous b), de la directive 95/46 »⁴³ (arrêt Schrems, §45), celle-ci rappelle, en se fondant sur le considérant 60 de la directive⁴⁴, que le caractère « complémentaire » du régime de transfert des

données vers les pays-tiers n'implique pas que ces transferts de données ne soient pas soumis aux conditions générales de licéité des traitements de données que doivent respecter les états-membres lorsqu'ils traitent des données sur leur territoire. Or, ce régime, prévu au Chapitre II de cette directive, est plus favorable aux droits fondamentaux des personnes (arrêt Schrems, §46).

- 19 Il était alors aisé d'étendre les pouvoirs des autorités nationales de contrôle au contrôle des transferts de données vers des pays tiers. En effet, dans la mesure où ces transferts doivent répondre au même niveau d'exigence de respect des droits fondamentaux que les traitements réalisés sur le territoire des Etats-membres d'une part, et que les autorités nationales doivent être investies des pouvoirs permettant de contrôler le respect de ces mêmes droits d'autre part. En conséquence, chacune de ces autorités doit être investie « de la compétence de vérifier si un transfert de données à caractère personnel depuis l'État membre dont elle relève vers un pays tiers respecte les exigences posées par la directive 95/46 » (arrêt Schrems, §49). Surtout, comme le rappelait l'avocat général, l'« impératif d'interprétation conforme aux droits fondamentaux » plaide en faveur d'une interprétation large des pouvoirs conférés aux autorités nationales de contrôle, car s'il en était autrement, les personnes dont les données ont été ou pourraient être transférées vers le pays tiers concerné seraient « privées du droit, garanti à l'article 8, paragraphes 1 et 3, de la Charte, de saisir les autorités nationales de contrôle d'une demande aux fins de la protection de leurs droits fondamentaux » (arrêt Schrems, §54 et 58)⁴⁵.

B - Une continuité temporelle de la protection des citoyens de l'Union

- 20 L'apport le plus spectaculaire de la décision ne réside toutefois pas dans la manière dont celle-ci fonde les exigences de contrôle indépendant des usages des données dans les garanties issues de l'article 8 de la Charte. Il est surtout remarquable que celle-ci, citant le « grand arrêt » Kadi (arrêt Schrems, §60), ancre l'accès effectif à un contrôle indépendant dans l'exigence d'accès à un recours effectif, indérogeable et spécifique à l'ordre juridique de l'Union qui, rappelle la Cour, est « une Union de droit dans laquelle tout acte de ses institutions est soumis au contrôle de la conformité [avec] les traités, les principes généraux du droit ainsi que les droits fondamentaux ». Un tel détour par l'arrêt Kadi n'est pas innocent. Rappelons que celui-ci avait, par un raisonnement radicalement dualiste, consacré une autonomie constitutionnelle par rapport aux décisions du Conseil de Sécurité, position au demeurant déjà adoptée s'agissant des rapports entre le droit de l'Union et le droit de l'OMC⁴⁶.
- 21 A cet égard, l'usage de l'arrêt Kadi prépare l'effet extraterritorial que confère la Cour au droit à la protection des données personnelles⁴⁷ : l'autonomie de « la charte constitutionnelle de base » que constituent les traités TFUE et TUE s'étend ici de manière remarquable à une norme extra-système, à savoir les normes de protection de la vie privée aux Etats-Unis. Ainsi énoncée, l'autonomie constitutionnelle du droit de l'Union ne fonde plus une simple « contre-limite » à l'introduction de normes externes dans l'ordre juridique de l'UE, mais également une véritable exigence d'« exportation » des normes de l'Union et du contrôle juridictionnel de la Cour de Justice. Puisque les données transférées vers des pays tiers doivent bénéficier d'un traitement similaire aux données traitées sur le territoire de l'UE d'une part et qu'internet constitue un espace

déterritorialisé et ubiquitaire d'autre part. Cela signifie très nettement que le droit à la protection des données personnelles a plus que jamais une portée mondiale – ce que visait précisément à éviter l'arrêt Lindqvist mais qu'avait déjà préfiguré la décision de la CJUE sur le « droit à l'oubli »⁴⁸.

- 22 Cette portée est d'autant plus forte si l'on se réfère aux conclusions conformes de l'avocat général, qui rappelait que les États membres doivent prévoir dans leur législation nationale que le transfert vers un pays tiers de données ne peut avoir lieu que « sous réserve du respect des dispositions nationales prises en application des autres dispositions de la directive 95/46, le pays tiers en question assure un niveau de protection adéquat »⁴⁹. Or, ces dispositions pouvant être plus favorables que celles prévues par la directive en raison de la marge de manœuvre des États membres⁵⁰, il est aisé de comprendre que les autorités nationales ont non seulement la possibilité de contrôler la compatibilité d'un transfert de données au regard de la directive, mais également de mesures nationales plus favorables, tant que celles-ci sont prises sur le fondement de la directive de 1995.
- 23 Ainsi énoncé, le droit de bénéficier d'un contrôle complet et indépendant n'est pas pour autant sans limites. En effet, si les juridictions nationales sont compétentes pour examiner la validité d'un acte de l'Union, elles n'ont en revanche pas compétence pour constater elles-mêmes l'invalidité d'un tel acte. Cela implique qu'une juridiction confrontée à une question relative à la validité d'un acte de droit tel qu'une décision de la Commission doit surseoir à statuer et saisir la Cour d'une procédure de renvoi préjudiciel en appréciation de validité, si les questions soulevées sont sérieux⁵¹ (arrêt Schrems, §62-64).
- 24 En outre, la continuité du contrôle est également assurée sur le plan territorial par le renforcement du contrôle de la Cour sur le niveau « adéquat » de protection des données personnelles dans les États-tiers. Toute en reconnaissant que le terme « adéquat » implique qu'il ne saurait être exigé qu'un tel pays assure un niveau de protection strictement identique à celui garanti dans l'ordre juridique de l'Union, celui-ci doit néanmoins être « substantiellement équivalent à celui garanti au sein de l'Union [...] » (arrêt Schrems, §73). Plus précisément, si les moyens auxquels ce pays tiers a recours peuvent être différents de ceux mis en œuvre au sein de l'Union, ceux-ci doivent être lus « de manière conforme aux droits fondamentaux », ce qui implique de procéder à un contrôle maximal au regard des exigences de la directive (arrêt Schrems, §74). A cet égard et comme le rappelait l'avocat général Yves Bot⁵², doivent être examinés de manière approfondie « le contenu des règles applicables et les moyens d'assurer le respect de ces règles ». Il doit donc exister dans le droit étranger en question un dispositif de contrôle externe sous la forme d'une autorité indépendante qui « constitue un élément nécessaire de tout système visant à assurer le respect des règles relatives à la protection des données à caractère personnel »⁵³. Un contrôle aussi approfondi a pour conséquence que la Cour doit analyser en profondeur le droit étranger – nord-américain en l'occurrence – en faisant usage de normes externes à celui-ci. Cela conduit ainsi à ériger la CJUE en nouveau juge « constitutionnel » du droit américain à la vie privée, sans pour autant que celle-ci ait, en pratique, l'autorité pour faire appliquer ses décisions.

C - Une continuité temporelle de la protection des citoyens de l'Union.

- 25 Est enfin consacrée une continuité temporelle de la protection des données personnelles des citoyens européens, car la constatation de l'existence d'un niveau de protection « adéquat » ne saurait faire obstacle au réexamen permanent de la compatibilité du Safe Harbor aux droits fondamentaux consacrés par le droit de l'Union, particulièrement lorsque des éléments de fait postérieurs tendant à démontrer que celui-ci. Citant longuement l'arrêt NS⁵⁴, la Cour comme l'avocat général Yves Bot⁵⁵ ont mené un raisonnement par analogie avec ledit arrêt. Pour parvenir à cette conclusion, la Cour se fonde ici sur l'architecture générale de la directive de 1995, notant que son article 28, n'a aucunement exclu du domaine de compétence des autorités nationales le contrôle des transferts de données vers des pays tiers. Surtout la Cour rappelle et confirme qu'une interprétation du droit dérivé qui reposerait sur une présomption irréfragable que les droits fondamentaux seront respectés – que ce soit par un État membre, par la Commission ou par un pays tiers – doit être considérée comme étant incompatible avec l'obligation des États membres, y compris lorsque les éléments de fait démontrant l'existence de l'atteinte sont postérieurs à la décision (arrêt Schrems, §77). En clair, la Cour réaffirme que le régime de transfert de données vers un État tiers ne saurait conduire à offrir aux citoyens une protection « au rabais » de leurs droits fondamentaux. Ce faisant elle assume le risque de renforcer l'effet extraterritorial du droit de l'Union et d'occasionner de sérieux conflits de normes.
- 26 Le raisonnement mené par la Cour, parsemé de références fortement axiologiques aux valeurs « constitutionnelles » de l'Union et de références plus pragmatiques aux révélations Snowden, semble avoir pour principale finalité de lever les contraintes juridiques restreignant les possibilités pour les citoyens européens de contester les usages de leurs données dans le cadre de la surveillance de masse. Elle conduit au surplus à conférer un effet extraterritorial au droit de l'Union et à multiplier spectaculairement les hypothèses dans lesquelles les citoyens peuvent remettre en cause – sur le plan juridictionnel – la surveillance de masse. Surtout, la Cour renforce son propre rôle en la matière en élargissant considérablement l'accès à son prétoire, s'ouvrant au discours de la société civile, ce qui pourrait à l'avenir avoir un impact sur la protection et la reconnaissance juridique du lancement d'alerte.
- 27 En cela, le raisonnement de la Cour de Luxembourg ressemble fort au raisonnement mené par la Cour de Strasbourg dans son arrêt Zakharov du 4 décembre 2015⁵⁶, qui a assoupli considérablement l'octroi du statut de « victime » au sens de l'article 34 de la convention ⁵⁷ aux personnes susceptibles d'être l'objet de mesures de surveillance sans pouvoir prouver que celles-ci ont effectivement été visées personnellement. Dans ce cadre, si les juges de Strasbourg avaient itérativement rappelé que le droit de saisine de la Cour n'offre pas de base à la contestation de violations de droits contenus dans la Convention et que les requérants doivent nécessairement avoir été « directement touchés » par le comportement ou la mesure qu'ils contestent, la Cour avait quelque peu assoupli sa jurisprudence pour l'adapter aux spécificités de la surveillance secrète. Dans l'arrêt Klass contre Allemagne, celle-ci avait ainsi énoncé que les individus peuvent, sous certaines conditions⁵⁸, bénéficier du statut de « victime » au sens de l'article sus-cité en raison de l'existence même de programmes de surveillance secrète, et sans avoir à prouver qu'ils

ont effectivement fait l'objet d'une telle surveillance. En effet, lorsqu'un Etat « instaure une surveillance secrète dont les personnes contrôlées ignorent l'existence et [...] demeure dès lors inattaquable », les droits consacrés par la convention pourraient se trouver réduits à néant⁵⁹.

- 28 Cette position avait été réaffirmée solennellement en 2010 dans l'arrêt Kennedy contre Royaume-Uni⁶⁰ où la Cour avait en outre clarifié les conditions dans lesquelles celle-ci peut être amenée à effectuer un contrôle in abstracto des législations relatives à la surveillance. Ainsi, pour savoir si un particulier peut se plaindre d'une ingérence du seul fait qu'il existe une législation autorisant des mesures de surveillance secrète, la Cour doit être attentive à la « l'accessibilité des recours en droit interne, et le degré de probabilité que les mesures de surveillance soient appliqués » aux requérants; plus particulièrement, lorsqu'il n'existe aucune possibilité de contester l'application de mesures de surveillance secrète en droit interne, les soupçons et les craintes de la population quant à l'usage abusif qui pourrait être fait des pouvoirs de surveillance secrète devraient être en principe justifiés, même lorsque « le risque de surveillance n'est guère élevé ».
- 29 Dans ce cas, la simple existence de lois et pratiques autorisant et instaurant un système de surveillance secrète des communications crée une menace de surveillance entravant forcément la liberté de communication et constituant en soi une ingérence dans l'exercice par les requérants de leurs droits découlant de l'article 8, quelles que soient les mesures prises à leur égard. Si cette présentation de la jurisprudence européenne a le mérite de la clarté, elle ne fait pas apparaître le caractère fluctuant de cette grille d'analyse. En effet, la Cour avait, à de multiples reprises, interprété de manière plus restrictive la portée de l'arrêt Klass contre Allemagne⁶¹, exigeant une « probabilité raisonnable » que les services de sécurité aient effectivement recueilli et conservé des informations sur la vie privée des requérants⁶².
- 30 Citant l'arrêt Digital Rights Ireland dans les « sources pertinentes » au regard de l'objet du litige, la Cour semble opter définitivement pour un accès large à son prétoire, ouvrant la voie à une à une multiplication des recours visant à contester in abstracto les législations européennes en la matière. Celle-ci énonce en effet que « l'approche Kennedy est la mieux adaptée à la nécessité de veiller à ce que le caractère secret des mesures de surveillance ne conduise pas à ce qu'elles [...] échappent au contrôle des autorités judiciaires nationales et de la Cour ». Toutefois, lorsqu'existent des recours effectifs en droit interne, l'individu doit alors « démontrer que sa situation personnelle le rend "potentiellement exposé au risque de subir pareilles mesures" (arrêt Zakharov, §171).

*

- 31 La décision de la Cour dans l'arrêt Schrems nous place bien loin de la situation qui prévalait dix ans auparavant, lorsque la Cour avait, dans son arrêt Lindqvist, insisté sur la spécificité du régime de transferts de données vers des pays-tiers pour éviter les conflits de normes. En effet, non seulement, l'indifférence de la Cour de Justice aux évolutions positives ayant eu lieu dans l'espace nord-américain et la référence par le juge Dedov à l'arrêt Clapper de la Cour Suprême des Etats-Unis⁶³ qui « n'a pas su aller assez loin »⁶⁴ dans l'élargissement de l'accès aux prétoires des citoyens démontrent que les décisions les plus récentes marquent la volonté d'affirmer l'identité au sens d'ipseité des valeurs européennes. Mais aussi, le contrôle opéré par la Cour l'a conduite à constater l'inconformité de cette décision aux droits fondamentaux de l'Union sur le double

fondement du droit à la protection des données personnelles mais également et surtout du droit à un recours juridictionnel effectif, qui s'effectue par une référence à l'arrêt Kadi et à l'« ordre constitutionnel européen »⁶⁵. Une telle montée en généralité s'opère en outre au profit d'une prise en compte croissante du discours de la société civile, la révélation de l'existence du programme « Prism » ayant joué un rôle de premier plan dans la décision de la Cour de réexaminer de manière approfondie la compatibilité aux droits fondamentaux de la décision 2000/520/CE puis de constater l'inconformité aux droits fondamentaux de l'Union des transferts de données transatlantiques, tandis que la décision de la Cour de Strasbourg d'assouplir l'accès au statut de « victime » en matière de surveillance des données n'est pas étrangère à l'existence d'une vision plus étroite de l'accès aux prétoires représentée par l'arrêt Clapper de la Cour suprême des Etats-Unis.

- 32 Une telle évolution, et l'extension aussi spectaculaire de son office - désormais extra-territorial - qui l'accompagne, ne sont pas le fruit du hasard, et s'expliquent par une rencontre fortuite entre le discours des opposants à la surveillance de masse d'une part, et le discours juridictionnel sur la constitutionnalisation de la Charte des droits fondamentaux d'autre part. En effet, la mise en œuvre d'un texte aussi « puissant et ouvert à l'interprétation »⁶⁶ permet à la Cour de contourner, en l'espèce, les contraintes juridiques liées à l'autorité du droit de l'Union et des décisions de la Commission en retenant une conception extensive de la protection des données personnelles. Cela lui permet de rejoindre le discours des opposants à la surveillance de masse et d'opérer une condamnation de celle-ci. A cet égard, l'élargissement de la compétence des autorités nationales de contrôle des données personnelles ne semble être qu'un « prétexte » pour instituer une triple continuité de la protection des données. Elle permet, en retour, de multiplier les possibilités pour les citoyens - et en particulier les militants - d'accéder aux prétoires via un système complexe de saisine de ces autorités suivie d'un renvoi par ces autorités de questions préjudicielles à la Cour. Et, par conséquent, de contribuer à la légitimation sociale de la Cour en instaurant un lien direct entre celle-ci et les citoyens.
- 33 En quelque sorte, le processus de constitutionnalisation du droit de l'Union ouvre la voie à une nouvelle « intertextualité », une nouvelle porosité entre le discours de la société civile et le discours juridictionnel sur les droits de l'homme. Cela libère la Cour de nombre de contraintes juridiques⁶⁷ et ouvre l'espace des possibles. Mais cela implique à tout le moins de placer une confiance énorme en la capacité de la Cour à assumer pleinement son rôle de gardien des droits fondamentaux dans l'ordre juridique de l'Union⁶⁸. Cette « intertextualité » nouvelle se double d'une porosité entre les jugements de la Cour de Luxembourg et celle de Strasbourg.
- 34 Une concurrence qui tend, en l'espèce, à renforcer la prohibition de la surveillance de masse.

*

2°/- Une prohibition renforcée de la surveillance de masse

- 35 Les motifs et les dispositifs de la décision Schrems ont pour conséquence une élévation spectaculaire du niveau d'exigence en matière de protection des données personnelles

des citoyens européens dont les données sont transférées vers les Etats-Unis. Surtout et puisque la décision Safe Harbor se contentait de reprendre des dispositions de droit américain, ses considérants constituent un constat officiel d'inconformité du système de surveillance de masse mis en place aux Etats-Unis. Au-delà, ses considérants constituent également un avertissement clair à l'égard des Etats-membres, de sorte que l'on assiste en la matière à la mise en place d'un véritable « ordre public » opposable sur le plan externe comme sur le plan interne à l'Union (A). Les arrêts Zakharov et Szabo rendus par la Cour Européenne des Droits de l'Homme vont, de manière remarquable, dans le même sens, celui d'une condamnation renforcée de la surveillance de masse (B).

A - La surveillance de masse vue de Luxembourg

- 36 Convoquant tour à tour les « grands arrêts » de la jurisprudence de la CJUE avec un appel insistant aux garanties « constitutionnelles » dont jouissent les justiciables de l'Union, le présent arrêt semble placé sous le signe heureux (?) de la constitutionnalisation du droit de l'Union. A ce titre, nombre de commentateurs l'ont comparé au désormais fameux arrêt Kadi, lui-même élevé au panthéon des « grands arrêts » du droit de l'Union⁶⁹. Ainsi, si l'arrêt Schrems se fonde sur l'arrêt Digital Rights Ireland⁷⁰ il complète et étend également la solution de cet arrêt. Comme l'avait souligné de manière pertinente le rapport « Numérique et droits fondamentaux » du Conseil d'Etat, les conséquences exactes à tirer de la décision Digital Rights restaient incertaines.
- 37 La Cour s'est précisément livrée à une interprétation « large » des considérants de l'arrêt Digital Rights Ireland, qu'elle vient compléter et renforcer. La prohibition de la surveillance de masse apparaît ainsi doublement fondée sur le droit à la protection des données personnelles et le droit à un recours effectif. Ce faisant, la Cour rappelle le strict caractère de précision, de nécessité et de proportionnalité que doivent revêtir ces atteintes. S'agissant de la précision, la Cour constate que consacre la primauté des « exigences relatives à la sécurité nationale, [à] l'intérêt public et [au] respect des lois des États-Unis » sur les principes de la sphère de sécurité, ce qui implique que les entreprises auto-certifiées recevant des données à caractère personnel depuis l'Union sont tenues « d'écarter ces principes lorsque ces derniers entrent en conflit avec ces exigences et s'avèrent donc incompatibles avec celles-ci » (arrêt Schrems, §86 et 87). Or, la généralité de cette dérogation autorise à porter largement atteinte à la vie privée sans qu'aucune limitation de ces atteintes ne soit définie, ni que soit précisé les cas dans lesquels la collecte de données peut intervenir – la référence à la sécurité nationale étant extrêmement large et imprécise.
- 38 À cet égard, il importe peu, pour établir l'existence d'une telle ingérence, que les informations relatives à la vie privée concernées présentent ou non un caractère sensible ou que les intéressés aient ou non subi d'éventuels inconvénients en raison de cette ingérence⁷¹. Or, une ingérence dans les droits fondamentaux garantis par les articles 7 et 8 de la Charte doit « prévoir des règles claires et précises régissant la portée et l'application d'une mesure et imposant un minimum d'exigences » notamment lorsqu'il existe un « risque important d'accès illicite à ces données »⁷² (arrêt Schrems, §91). Surtout, raisonnant par analogie avec l'arrêt Digital Rights, la Cour rappelle que la simple l'existence de législations autorisant la mise en œuvre de mesures de surveillance sans qu'aucune « différenciation, limitation ou exception » ne soit opérée en fonction de l'objectif poursuivi et sans qu'aucun critère objectif permette de délimiter l'accès des

autorités publiques aux données et leur utilisation ultérieure, constitue une violation grave de la protection des données personnelles (arrêt Schrems, §93). Enfonçant le clou, la Cour estime ainsi qu'une telle réglementation permettant « d'accéder de manière généralisée au contenu de communications électroniques » porte nécessairement atteinte au contenu essentiel de ces droits fondamentaux, tel que garantis par les articles 7 et 8 de la Charte (Arrêt Schrems, §94).

- 39 L'absence de précision et de nécessité des atteintes à la vie privée autorisées par le Safe Harbor n'était pas le seul grief adressé à ce système : au-delà de l'étendue massive de l'ingérence dans les données, c'est surtout l'absence totale de possibilité de recours effectif qui préoccupe la Cour. En effet, si celle-ci ne condamne pas dans son principe le système d'auto-certification, elle rappelle néanmoins que celui-ci ne peut être considéré comme valide que dans la seule mesure où des « mécanismes efficaces de détection et de contrôle permettant d'identifier et de sanctionner de manière efficace des atteintes au droit à la vie privée et à la protection des données personnelles » (Arrêt Schrems, §89). Or, précisément, l'avocat général avait rappelé dans ses conclusions que ni la FTC ni les organismes d'arbitrage privé n'ont donc de « compétence pour contrôler les possibles violations des principes de protection des données à caractère personnel commises par des acteurs publics tels que les agences de sécurité américaines »⁷³. En effet, la première n'est compétente que pour les actions et les pratiques déloyales ou frauduleuses dans le domaine du commerce, les seconds ne pouvant pas, pour leur part, traiter de telles violations qui sont commises « par des organismes ou des autorités autres que les entreprises auto-certifiées ».
- 40 Dans les deux cas, aucune des deux instances n'ont compétence pour statuer sur la légalité des activités des agences de sécurité américaines, et leur rôle n'est aucunement comparable à celui des autorités nationales de contrôle prévues à l'article 28 de la directive 95/46. Ainsi en étant limité aux litiges commerciaux, le contrôle de la FTC est impuissant à faire constater l'existence d'atteintes au droit à la protection des données personnelles commis par des agences de sécurité.
- 41 Or, la possibilité d'obtenir l'effacement et la rectification des données personnelles indûment traitées figure explicitement dans le libellé de l'article 8 de la Charte et constitue désormais une exigence conditionnant le respect du contenu même du droit fondamental à la vie privée. En effet, la Cour a souligné itérativement la nécessité de se fonder sur une interprétation de la directive 95/46/CE permettant d'assurer un juste équilibre entre les différents droits et libertés fondamentaux protégés par l'ordre juridique de l'Union⁷⁴ dans lequel le droit à la vie privée garanti par la Convention européenne revêt une signification particulière⁷⁵. Cette recherche d'une interprétation de la directive conforme aux droits fondamentaux a, par le passé, conduit le juge de Luxembourg à fonder le droit à l'effacement sur les articles 7 et 8 de la Charte. Dans l'arrêt Google Spain, la Cour a en effet qu'une personne peut demander l'effacement de données publiques devenues non pertinentes non pas uniquement au regard des articles 12 et 14 de la directive de 1995, mais plus largement et « eu égard à ses droits fondamentaux » au titre de ces dispositions de la Charte⁷⁶. Cela signifie que les mécanismes institués par les articles 12 et 14 de la directive ont désormais un ancrage direct dans la CDFUE.
- 42 La Cour de justice, de manière remarquable, va bien plus loin encore dans l'arrêt en convoquant les « grands arrêts » du droit de l'Union sur le droit au recours effectif⁷⁷. Elle énonce qu'une réglementation ne prévoyant aucune possibilité pour le justiciable

d'exercer des voies de droit afin d'avoir accès à des données à caractère personnel le concernant, ou d'obtenir la rectification ou la suppression de telles données, ne respecte pas le contenu essentiel du droit fondamental à une protection juridictionnelle effective consacré à l'article 47 de la CDFUE. À cet égard, l'existence même d'un contrôle juridictionnel effectif destiné à assurer le respect des dispositions du droit de l'Union est inhérente à l'existence d'un État de droit⁷⁸. La prohibition de la surveillance de masse, fondée depuis 2014 sur le droit à la protection des données personnelles et le droit à la protection de la vie privée, est donc désormais ancré dans les exigences conçues par la Cour comme « inhérentes à l'existence d'un Etat de droit ».

B - La surveillance de masse vue de Strasbourg

- 43 La Cour de Strasbourg a adopté le même type de position sous l'angle de l'article 8 de la CEDH. En effet, dans un arrêt Sakharov, la Cour a, sans opérer de revirement de jurisprudence en la matière, exercé un sévère encadrement de la surveillance dite « de masse ». Rappelant la série des arrêts Rotaru⁷⁹, S. et Marper⁸⁰ et Kennedy⁸¹, les juges de Strasbourg ont rappelé les exigences de qualité, de précision et de nécessité que doit remplir une législation pour passer le cap du contrôle opéré par la Cour. En tout premier lieu, ce type de loi doit être accessible à la personne concernée et prévisible quant à ses effets⁸² et, si cette exigence de prévisibilité et d'accessibilité de la loi n'a pas la même portée en matière de surveillance secrète, celle-ci doit en revanche être a minima rédigée avec suffisamment de clarté pour permettre aux individus de savoir « en quelles circonstances et sous quelles conditions elle habilite la puissance publique à prendre pareilles mesures secrètes »⁸³. En second lieu, la loi doit « définir l'étendue et les modalités d'exercice d'un tel pouvoir [de surveillance secrète] » et préciser la nature des infractions susceptibles d'être couverte, mais également - nous citons in extenso - « la définition des catégories de personnes susceptibles d'être mises sur écoute, la fixation d'une limite à la durée d'exécution de la mesure, la procédure à suivre pour l'examen, l'utilisation et la conservation des données recueillies, les précautions à prendre pour la communication des données à d'autres parties, et les circonstances dans lesquelles peut ou doit s'opérer l'effacement ou la destruction des enregistrements »⁸⁴.
- 44 Sur un plan plus substantiel, la loi doit également être « nécessaire dans une société démocratique » à la réalisation d'un but légitime. A cet égard, si la Cour a reconnu de longue date que si les Etats-membres disposent « d'une certaine marge d'appréciation dans le choix des moyens propres à atteindre le but légitime que constitue la protection de la sécurité nationale », celle-ci n'est en aucun cas un blanc-seing accordé à ces mêmes autorités, les juges devant s'assurer de l'existence de « garanties adéquates et effectives contre les abus »⁸⁵. Cet examen doit en principe être complet et intervenir à trois stades, pour assurer un contrôle de l'ensemble des abus que peut susciter ce type de surveillance : lorsque celle-ci est ordonnée, lorsque celle-ci est menée, et lorsque celle-ci a pris fin⁸⁶.
- 45 Faisant application de ces principes, la Cour a conclu que les dispositions du droit russe régissant l'interception de communications ne « comportent pas de garanties adéquates et effectives contre l'arbitraire et le risque d'abus inhérent à tout système de surveillance secrète » (arrêt Zakharov, §302). Il est particulièrement intéressant d'aborder brièvement les raisons ayant conduit la Cour à condamner le système russe car, comme le souligne à juste le Professeur Woods⁸⁷, il apparaît clairement que la portée du jugement Zakharov

dépasse les enjeux de l'affaire et constitue un signal à l'intention d'autres Etats parties à la Convention, en particulier ceux dont les lois sur le renseignement sont contestées devant les prétoires strasbourgeois.

- 46 En premier lieu, la Cour a fait grief à la législation russe de ne pas avoir énoncé avec suffisamment de précision les circonstances dans lesquelles les pouvoirs publics sont habilités à recourir aux mesures de surveillance. Rappelant que des « menaces dirigées contre la sécurité nationale peuvent être de différentes natures et peuvent être imprévues ou difficiles à définir à l'avance »⁸⁸ mais que la loi irait à l'encontre de la « prééminence du droit » si le pouvoir d'appréciation accordé à l'exécutif en matière de sécurité nationale ne connaissait pas de limite. Elle fait aussi grief à la législation russe de ne donner aucune indication sur « les circonstances dans lesquelles les communications d'une personne peuvent être interceptées en raison de faits ou d'activités qui mettent en péril la sécurité nationale, militaire, économique ou écologique [...] », ce qui confère aux autorités une « latitude quasi illimitée » (arrêt Zakharov, §248). Toutefois, elle relève que le fait que ces mesures soient ordonnées par un juge constituait une garantie importante contre l'arbitraire.
- 47 C'est surtout l'absence d'effectivité du contrôle qui préoccupe la Cour en l'espèce. S'agissant en effet du contrôle des mesures de surveillance, les juges rappellent certes que la délivrance d'autorisations d'effectuer des écoutes téléphoniques par un service non judiciaire peut être compatible avec la Convention⁸⁹. Mais il importe à cet égard que l'organisme de contrôle soit suffisamment indépendant à l'égard de l'exécutif⁹⁰ et dispose de tous les pouvoirs nécessaires s'assurer que l'interception des données présente un caractère de nécessité et de proportionnalité au regard des buts poursuivis « en vérifiant par exemple s'il est possible d'atteindre les buts recherchés par des moyens moins restrictifs »⁹¹ (arrêt Zakharov, §260).
- 48 Or, le système russe n'instaurait qu'un contrôle de portée limitée : des informations essentielles telles que l'organisation et la tactique mise en œuvre pour surveiller les individus ne peuvent être soumis au juge. En outre, les pouvoirs de l'organe de contrôle relativement aux infractions qu'il peut déceler, qui constituent « un aspect important pour l'appréciation de l'effectivité du contrôle qu'il exerce » (arrêt Zakharov, §282)⁹² Or, si les procureurs disposent d'un tel pouvoir en Russie, la Cour avait d'ores et déjà dénié les qualités d'indépendance à un ministère de l'intérieur directement impliqué dans la commande de moyens spéciaux de surveillance et à un procureur général et des procureurs de rang inférieur compétents⁹³. Elle juge en l'espèce que les modalités de nomination des procureurs russes conduit à « susciter des doutes quant à leur indépendance à l'égard de l'exécutif » (arrêt Zakharov, §279). Enfin, l'effectivité des recours est compromise par l'absence de notification des interceptions à un stade quelconque, ou d'un accès approprié aux documents relatifs aux interceptions (arrêt Zakharov, §302). La Cour est sensiblement parvenue aux mêmes conclusions et pour des raisons similaires dans son plus récent arrêt Szabo, faisant notamment grief à la législation hongroise de ne soumettre le contrôle a posteriori des mesures de surveillance qu'à une instance politique, le ministère de la Justice.
- 49 Si l'arrêt Zakharov ne concerne stricto-sensu que des mesures de surveillance ciblées et ne porte pas sur le cas spécifique de l'interception de toutes les données à tout moment, celui-ci condamne a fortiori ce type de surveillance, comme en témoigne là aussi l'affaire Szabo⁹⁴. Dans ce dernier arrêt, la Cour note non seulement que la législation hongroise « peut potentiellement affecter tout le monde et, qu'à ce titre, elle peut être interprétée

comme ouvrant la voie à la surveillance illimitée d'un grand nombre de citoyens ». Elle énonce aussi que ces mesures ne peuvent être mises en œuvre qu'en cas de stricte nécessité liée à la sauvegarde des institutions démocratiques et à l'obtention de renseignement par le biais d'une opération individuelle (arrêt Szabo, §67)⁹⁵.

Conclusion : Grandeur et ambiguïtés de la condamnation de la surveillance de masse

- 50 Les trois décisions commentées placent désormais l'ensemble des cours européennes, mais également des cours nord-américaines, face à leurs responsabilités s'agissant du contrôle de législations instaurant une surveillance pouvant être considérée comme abusive. S'agissant de la condamnation de la surveillance « de masse », la décision Schrems, mise en perspective avec la décision Zakharov du 4 décembre 2015 et la décision Szabo du 12 janvier 2016, renforce en effet de manière inédite les garanties accordées aux citoyens européens contre les abus de la surveillance secrète. Elle fonde la prohibition de la surveillance de masse sur une double garantie tirée d'une part du droit à la protection des données personnelles mais également – et de manière plus novatrice – sur le droit à un recours effectif. En résulte d'une part une élévation du niveau de précision dont doivent faire preuve les lois instituant une surveillance secrète, mais également un élargissement très net de l'accès aux prétoires strasbourgeois et luxembourgeois d'autre part.
- 51 En cela, les deux décisions placent très nettement la protection des données sous le signe du droit au recours effectif et, plus largement, de la prééminence du droit. Il apparaît en effet que les décisions commentées marquent bien une maturation du discours des juges européens, qui n'est désormais plus uniquement axé sur la précision et la nécessité des lois instaurant une surveillance, mais surtout et avant tout sur la nécessité de prévoir un contrôle effectif des excès de telles lois. En cela, les décisions de la CJUE et de la CEDH marquent clairement la prise en compte des révélations Snowden et, surtout, des prises de position de l'Union européenne⁹⁶, du Conseil de l'Europe⁹⁷ et de l'ONU⁹⁸ qui, citées dans les arrêts Zakharov et Szabo dans les « sources pertinentes » au regard de l'objet du litige, avaient précisément insisté sur la nécessité de prévoir un contrôle juridictionnel effectif.
- 52 La « nouvelle approche » de ces cours en la matière – qui certes était déjà en germe depuis bien longtemps – ne saurait être mieux résumée que par l'opinion concordante du juge Bulgare (le juge Dedov) dans l'arrêt Zakharov. Celui-ci estimait que l'appréciation large de cet arrêt de la condition de victime pourrait servir à « une amélioration de la législation en matière de mesures opérationnelles d'investigation et à l'établissement d'un système effectif de contrôle public sur la surveillance ». Et cela notamment lorsqu'il « n'y a pas d'autres moyens disponibles pour protéger la démocratie et la prééminence du droit ». Citant Edward Snowden en conclusion, il rappelle qu'il s'agit là d'un rôle que le juge « se doit de jouer dans la société civile », sous entendant clairement que l'arrêt Zakharov n'a d'autre but que d'instaurer plus aisément un dialogue direct avec les citoyens lorsque les cours nationales n'effectuent pas un contrôle effectif des excès de la surveillance.
- 53 Cette nouvelle vision n'est néanmoins pas dépourvue d'ambiguïtés. Plus qu'une condamnation stricte de la surveillance de masse, il semble plausible que les réponses des juges européens constituent une pratique une reconnaissance de l'inéluctabilité du développement de celle-ci, dont les effets devraient alors être contre-balancés par un

contrôle effectif des cours sur les abus d'une surveillance de ce type. En effet, comme certains défenseurs des droits de l'homme l'ont remarqué, le considérant 69 de la décision Szabo indique que la Cour « admet que les formes prises par le terrorisme de nos jours ont pour conséquence naturelle un recours par les gouvernements à des technologies de pointe, notamment à des techniques de surveillance massive des communications, afin d'éviter des incidents imminents » et que la priorité est désormais d'instaurer un contrôle effectif sur ces lois.

- 54 Une telle conclusion pourrait fort bien être confortée par le fait que l'arrêt Schrems fonde une véritable exigence d'exportation du contrôle indépendant « à l'Européenne » dans le système américain. Or, la Cour de Luxembourg ne peut ignorer que le fait accorder de manière croissante une portée extraterritoriale au droit de l'Union conduira rapidement à une impasse, comme le démontre d'ailleurs l'annonce récente de la négociation d'un « Privacy Shield » dans lequel l'on a peine à voir en quoi il se distingue du désormais défunt Safe Harbor⁹⁹. Il est vrai que la rigueur de la condamnation de la surveillance de masse aux Etats-Unis opérée par l'arrêt Schrems laisse forte peu de marge de manœuvre aux autorités Européennes et Nord-Américaines pour négocier une porte de sortie, de sorte que la controverse transatlantique sur ce point ne risque pas de se clore¹⁰⁰. En effet, si la position du G29 et la foire aux questions (FAQ) publiée par la Commission européenne¹⁰¹ font référence aux clauses contractuelles types et au recueil du consentement des personnes, il paraît peu probable que les solutions adoptées puissent constituer une porte de sortie acceptable. Comme le souligne à juste titre Steve Peers¹⁰², la référence par la Cour aux exigences du droit primaire rend illusoire une sortie de conflit par le biais de la révision en cours de la protection des données personnelles : seule une nouvelle décision Safe Harbor pourrait tenir lieu de mise en conformité avec l'arrêt Schrems.
- 55 Or, puisque la portée de cet arrêt conduit à considérer tout système de surveillance de masse comme une violation en soi du contenu essentiel de la vie privée. Seule une réforme du système de surveillance américain conduisant doublement à instaurer une surveillance ciblée et à mettre en place un contrôle indépendant pourrait permettre de relancer les échanges de données transatlantiques : nous sommes ici bien loin du compte ! Faute de pouvoir être suivie d'effets concrets dans un futur proche, gageons que la montagne accouchera d'une souris et que la Cour sera dans l'obligation de modérer sa position. Constatons donc que le processus de constitutionnalisation des droits fondamentaux de l'Union européenne nous renvoie, une fois de plus, à la désormais célèbre difficulté « contre-majoritaire » : celle de cours constitutionnelles - ou supposées telles - qui, « exerçant un contrôle non pas au titre de la majorité dominante, mais contre celle-ci. [...] ¹⁰³ » se voient en permanence soumises à un impératif majeur de légitimation.

*

- 56 CJUE, Gr.Ch., 6 octobre 2015, Maximilian Schrems c. Data Protection Commissioner, Aff. C-362/14
- 57 Cour. EDH, Gr. Ch., 4 décembre 2015, Zakharov c. Russie, Req. n°47143/06
- 58 Cour EDH, 5e sect., 12 janvier 2016, Szabo c. Hongrie, Req.n°37138/14

*

Les Lettres « Actualités Droits-Libertés » (ADL) du CREDOF (pour s'y abonner et se désabonner) sont accessibles sur le site de la Revue des Droits de l'Homme (RevDH) – Contact

NOTES

1. Edward Snowden, "Pendant que vous lisez ceci, le gouvernement en prend note", Libération, Tribunes, 6 juin 2015.
2. Isabelle Boucoba et Charlotte Girard, « « Constitutionnaliser » l'état d'urgence ou comment soigner l'obsession d'inconstitutionnalité ? », La Revue des droits de l'homme [En ligne], Actualités Droits-Libertés, mis en ligne le 05 février 2016 ; Rapport L'urgence d'en sortir, Analyse approfondie du régime juridique de l'état d'urgence et des enjeux de sa constitutionnalisation dans le projet de loi dit « de protection de la nation », Janvier 2016 ; Arnaud Gossement, « La constitutionnalisation de l'état d'urgence : juridiquement justifiable, politiquement contestable », Blog Médiapart, 23 décembre 2015.
3. V., notamment : Congressional Research Service, NSA Surveillance Leaks: Background and Issues for Congress, 4 septembre 2013 ; D. Bigo, S. Carrera, N. Hernanz *et al.*, « Mass Surveillance of Personal Data by EU Member States and its Compatibility with EU Law », *Liberty and Security in Europe Papers*, 2013, no 61
4. CJUE, Grande Chambre, 8 avril 2014, *Digital Rights Ireland Ltd & Michael Seitlinger e.a.*, affaires jointes C-293/12 & C-594/12. V. Florence Benoit-Rohmer, « Protection des données personnelles ; Note sous Cour de justice de l'Union européenne, grande Chambre, 8 avril 2015, Digital Rights Ireland Ltd contre Minister for Communications, Marine and Natural Resources et autres et Kärnter Landesregierung Seitlinger et autres, affaires jointes numéros C-293/12 et C-594/12 », *RTDE* 2015, p.168 Denys Simon, « La révolution numérique du juge de l'Union : les premiers pas de la cybersociété », *Europe* n°7, p.4 ; Marie-Laure Basilien-Gainche, « Une prohibition européenne claire de la surveillance électronique de masse », in *Revue des droits de l'homme*, 14 mai 2014
5. UK High Court, "David Davis and others -v- Secretary of State for the Home Department", 17 juillet 2015
6. H.R. 2048, Pub.L. 114-23
7. V. Spencer Ackerman, 17 April 2015). "Weakened surveillance reform bill is 'yesterday's news', civil libertarians say". The Guardian, 17 avril 2015; Stephanie Condon . "NSA surveillance reform bill now law". CBS News, 2 juin 2015 ;
8. V. Mireille Delmas-Marty et Marie-Laure Izorche, "Marge nationale d'appréciation et internationalisation du droit. Réflexions sur la validité formelle d'un droit commun pluraliste." *Revue internationale de droit comparé*, 2000, vol. 52, no 4, p. 753-780.
9. Cour. EDH, Gr. Ch., 4 décembre 2015, Zakharov c. Russie, Req. n°47143/06
10. Cour EDH, 5e sect., 12 janvier 2016, Szabo c. Hongrie, Req. n°37138/14
11. V. Owen Bowcott, "Data retention powers referred to european court", The Guardian, 20 novembre 2015 ; V. Également les deux requêtes pendantes suivantes : Big brother watch et autres c. Royaume-Uni (no 58170/13) ; Bureau of investigative journalism and Alice Ross c. Royaume-Uni (n°62322/14)

12. V. sur ce paradigme : Paul De Hert et Serge Gutwirth. "Data protection in the case law of Strasbourg and Luxembourg: Constitutionalisation in action." (2009): 3-44.
13. Et ce en prenant en compte « la nature des données, la finalité et la durée du ou des traitements envisagés, les pays d'origine et de destination finale, les règles de droit, générales ou sectorielles, en vigueur dans le pays tiers en cause, ainsi que les règles professionnelles et les mesures de sécurité qui y sont respectées ».
14. Décision 2004/915/CE du 27 décembre 2004, modifiant la décision 2001/497/CE en ce qui concerne l'introduction d'un ensemble alternatif de clauses contractuelles types pour le transfert de données à caractère personnel vers de pays tiers [Journal officiel L 385 du 29.12.2004].
15. Voir, pour une comparaison des deux systèmes : David L., Baumer, Julia B. Earp et J. C. Poindexter, "Internet privacy law: a comparison between the United States and the European Union", *Computers & Security*, 2004, vol. 23, no 5, p. 400-412.
16. Yves Pouillet, "Les Safe Harbor Principles-Une protection adéquate", *Conférence de l'IFCLA "Le droit de l'informatique au tournant du millénaire"*, Paris. 2000.
17. G29, WP 12: "Transferts de données personnelles vers des pays tiers: application des articles 25 et 26 de la directive communautaire sur la protection des données", document adopté le 24 juillet 1998 par le groupe de travail. ; WP 15: Avis 1/99 concernant le niveau de protection des données à caractère personnel aux États-Unis et les discussions en cours entre la Commission européenne et le gouvernement américain ; WP 19: Avis 2/99 concernant la pertinence des "principes internationaux de la 'sphère de sécurité'" publiés par le ministère du commerce des États-Unis le 19 avril 1999 ; WP 21: Avis 4/99 concernant les questions souvent posées, devant être publiées par le ministère américain du commerce dans le cadre des principes proposés pour la "sphère de sécurité".
18. V. pour plus de détails : Congressional Research Service, "The EU-U.S. Safe Harbor Agreement on Personal Data Privacy: In Brief", 29 octobre 2015 ; "The Federal Trade Commission's Regulation of Data Security under Its Unfair or Deceptive Acts or Practices (UDAP) Authority", 11 septembre 2014.
19. Congressional Research Service, "Online Data Collection and Disclosure to Private Entities: Selected Federal Laws and Self-Regulatory Regimes", 1er avril 2011.
20. Commission Européenne, « L'application de la décision 2000/520/CE de la Commission, du 26 juillet 2000, conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à la pertinence de la protection assurée par les principes de la « sphère de sécurité » et par l», SEC (2002) 199, 13 décembre 2002.
21. Commission Européenne « La mise en œuvre de la décision 2000/520/CE de la Commission relative à la pertinence de la protection assurée par les principes de la « sphère de sécurité » et par les questions souvent posées y afférentes, publiés par le ministère du commerce des États-Un », SEC(2004) 1323, 20 octobre 2004.
22. Chris Connolly (Galexia), « US Safe Harbor - Fact or Fiction? Privacy Laws and Business International, issue 96, December 2008 », published on Galexia.com, retrieved 30 October 2015.
23. V. Nikolaj Nielsen, "Hundreds of U.S. Companies Make False Data Protection Claims," EUObserver.com, October 8, 2013; Nikolaj Nielsen, "Leading EU Party Wants to Ditch U.S.-EU Data Protection Agreement," EUObserver.com, October 29, 2013.
24. Joris Van Hoboken, Nico Axel van Eijk, "Cloud Computing in Higher Education and Research Institutions and the USA Patriot Act", 27 novembre 2012.
25. Considérant notamment que « sphère de sécurité sert également d'interface pour le transfert de données à caractère personnel de citoyens européens, de l'[Union] vers les

États-Unis, par les entreprises qui sont tenues de remettre des données aux agences américaines de renseignement dans le cadre de programmes américains de collecte de renseignements. V. Commission Européenne, « Communication au parlement européen et au conseil relative au fonctionnement de la sphère de sécurité du point de vue des citoyens de l'union et des entreprises établies sur son territoire », COM(2013) 847 final, 27 novembre 2013.

26. M. Shrems n'était en effet pas en mesure de prouver que ses données avaient été, dans les faits, collectées et utilisées par la NSA. V., Steve Peers, " Europe v Facebook: the beginning of the end for NSA spying on EU citizens ?", EU Law analysis, 18 juin 2014.

27. Steve McGarr, "Do Facebook and the USA violate EU data protection law? The CJEU hearing in Schrems ", EU Law analysis, 29 mars 2015.

28. V. High Court (Irlande), "Maximilian Schrems v. Data Protection Commissioner", 18 juin 2014

29. V. Conseil d'Etat, Etude annuelle 2014, Le numérique et les droits fondamentaux, adoptée le 17 juillet 2014 par l'assemblée générale du Conseil d'Etat, publiée le 9 septembre 2014, p.153.

30. Steve McGarr, "Do Facebook and the USA violate EU data protection law? The CJEU hearing in Schrems ", EU Law analysis, 29 mars 2015.

31. CJUE, 5 octobre 2004, Commission c/ Grèce, Aff. C-475/01, §18 ; 15 juin 1994, Commission c/ BASF e.a., Aff. C-137/92 P, 48, 8 juillet 1999, Chemie Linz c/ Commission, C-245/92 § 93.

32. Obituary: Lord MacKenzie-Stuart', The Guardian, 25 Mai 2000. Cité dans : Christopher Vajda, « The Application of the EU Charter of Fundamental Rights: Neither Reckless nor Timid? », 18 novembre 2014, Edinburgh School of Law Research Paper No. 2014/47.

33. CJUE, Gr.Ch., 6 octobre 2015, Maximilian Schrems c. Data Protection Commissioner, Aff. C-362/14, §35.

34. CJUE, Grande Chambre, 13 mai 2014, *Google Spain SL et Google Inc. c. Agencia Española de Protección de Datos et Mario Costeja González*, Aff. C-131/12 – Communiqué de presse et ADL du 16 juin 2014.

35. CJCE, 20 mai 2003, Österreichischer Rundfunk e.a. , Aff. C-465/00 § 64 ; CJUE, GC, 13 mai 2014, *Google Spain SL et Google Inc. c. Agencia Española de Protección de Datos et Mario Costeja González*, préc., §68

36. CJUE, 24 novembre 2011, ASNEF et FECEMD, Aff. C-468/10 et C-469/10 , § 38 et 40 ; V. Conclusions de l'avocat général M. Niilo Jääskinen, 17 novembre 2011, *Bonnier Audio AB contre Perfect Communication Sweden AB («ePhone»)*, Affaire C-461/10, § 54

37. CJUE, 16 octobre 2012, Commission/Autriche, Aff. C-614/10, §36, ; CJUE, 8 avril 2014 Commission/Hongrie C-288/12, §47. V., sur les derniers développements en la matière : Steve Peers, « The CJEU confirms the independence of data protection authorities », EU Law Blog, 9 avril 2014. Voir également, pour une analyse plus large de ces arrêts : Fabienne Kauff-Gazin, « Vers une conception européenne de l'indépendance des autorités de régulation ? - À propos de l'affaire C-518/07, Commission c/ Allemagne », Europe - Juillet 2010 - n° 7.

38. CJUE, 9 mars 2010, Commission/Allemagne, Aff. C-518/07 §24, ; CJUE, 8 avril 2014 Commission/Hongrie C-288/12, §51.

39. V. En ce sens : Miguel Poiars Maduro, "Interpreting European Law-Judicial Adjudication in a Context of Constitutional Pluralism", 2008.

40. CJUE, 6 novembre 2003, Lindqvist, aff. C-101/01, Rec. p. I-12971, §63 ; V. Gloria Gonzalez-Fuster et Serge Gutwirth, "Privacy 2.0?" *Revue du droit des Technologies de l'Information*, 2008, p. 349-359.
41. V. Andreas Busch, « From Safe Harbour to the rough sea? Privacy disputes across the Atlantic " *SCRIPT-ed*, 2006, vol. 3, no 4.
42. V. Steve Peers, « The party's over: EU data protection law after the Schrems Safe Harbour judgment », *EU Law Analysis*, 7 octobre 2015.
43. CJUE, 30 mai 2006, Parlement c. Conseil et Commission, Aff. C-317/04 et C-318/04, EU:C:2006:346, §56.
44. « Considérant que, en tout état de cause, les transferts vers les pays tiers ne peuvent être effectués que dans le plein respect des dispositions prises par les États membres en application de la présente directive, et notamment de son article 8 ».
45. V., dans le même sens : CJUE, Grande Chambre, 8 avril 2014, *Digital Rights Ireland Ltd & Michael Seitlinger e.a.*, aff. j. C-293/12 & C-594/12, §68.
46. V. not. Jean-Claude Zarka, « Absence d'effet direct eds règles de l'OMC dans l'ordre juridique communautaire », *JCP / La semaine juridique*, n° 30, 27 juillet 2005, 10106. - G.A. Zonnenkeyn « EC liability for non-implementation of WTO dispute settlement decisions – are the dice cast ? », *Journal of International Economic Law*, 7 (2), 2004, p. 483-490.
47. V. sur le développement de l'extraterritorialité du droit de l'Union : Joanne Scott, " Extraterritoriality and territorial extension in EU law", *American Journal of Comparative Law*, 2014, vol. 62, no 1, p. 87-125 ; "The New EU' Extraterritoriality", *Common Market Law Review*, 2014, vol. 51.
48. V. Spiros Tassis et Margarita Periseraki, "The Extraterritorial Scope of the Right to Be Forgotten and How This Affects Obligations of Search Engine Operators Located outside the EU", *Eur. Networks L. & Reg. Q.*, 2014, p. 244.
49. Conclusions de l'avocat général Yves Bot sur l'Affaire C-362/14, « Maximilian Schrems c. Data Protection Commissioner », §76
50. CJUE, Troisième chambre, 7 novembre 2013, IPI, Aff. C473-12, §32.
51. CJUE, 28 avril 2015, T & L Sugars et Sidul Açúcares/Commission, C-456/13 P, EU:C:2015:284, §48 ; CJUE, 28 octobre 1987, Foto-Frost, Aff. 314/85, §15 à 20 ; CJUE, 10 janvier 2006, IATA et ELFAA, Aff. C-344/04, § 27.
52. Conclusions de l'avocat général Yves Bot sur l'affaire C-362/14, préc., §52
53. *Ibid.*
54. Cet arrêt avait jugé, dans le contexte du régime européen d'asile où il doit être présumé que le traitement réservé aux demandeurs d'asile dans chaque État membre est conforme aux exigences de la Charte mais que cette présomption est réfragable lorsque peuvent êtres constatées des défaillances systémiques de la procédure d'asile pouvant sérieusement soumettre les demandeurs d'asile à des conditions d'accueil attentatoires à leur dignité. V. CJUE, 21 décembre 2011, NS e.a., Aff. C-411/10
55. Concl. préc.
56. Cour. EDH, Gr. Ch., 4 décembre 2015, Zakharov c. Russie, préc.. V. Lorna Woods, "Zakharov v Russia: Mass Surveillance and the European Court of Human Rights", *EU Law Analysis*, 16 décembre 2015.
57. V. Cour EDH, Service de Presse, Guide pratique sur la recevabilité, 2014.
58. Klass, préc.
59. *Ibid.*

60. Cour EDH, 4^e Sect. 18 mai 2010, Kennedy c. Royaume-Uni, Req. n° 26839/05 – ADL du 20 mai 2010.
61. Klass, préc.
62. Cour EDH, 25 juin 1997, Halford c. Royaume-Uni, Req. no 20605/92, §47 ; Cour EDH, 22 juin 2006 Weber et Saravia c. Allemagne, no. 54934/00, §§ 4-6 et 78 ; Cour EDH, 4^e Sect. 18 mai 2010, Kennedy c. Royaume-Uni, préc. V. Plus largement : Cour EDH, Division de la recherche, “Sécurité nationale et jurisprudence européenne”, 2013.
63. V. Lorna Woods, "Zakharov v Russia: Mass Surveillance and the European Court of Human Rights", EU Law analysis, 16 décembre 2015
64. "In contrast, in the case of Clapper v. Amnesty International USA (568 U.S. ____ (2013), the US Supreme Court failed to take a step forward, despite the existence of a mass surveillance programme and “the widespread suspicion” of its existence. Instead, it rejected as insufficient the argument by the plaintiffs (including human-rights, legal and media organisations) that they were likely to be subject to surveillance due to the nature of their work.” V. Cour. EDH, Gr. Ch., 4 décembre 2015, Zakharov c. Russie, Req. n° 47143/06 ,Opinion séparée mais concordante du juge Dedov.
65. V. En ce sens : Elena Simina Tanescu, "Rôle des droits fondamentaux dans la constitutionnalisation de l'ordre juridique de l'UE", in *The Court of Justice and the Construction of Europe: Analyses and Perspectives on Sixty Years of Case-law-La Cour de Justice et la Construction de l'Europe: Analyses et Perspectives de Soixante Ans de Jurisprudence*. TMC Asser Press, 2013. p. 207-227.
66. David Anderson et Cian Murphy, »The Charter of Fundamental Rights: History and Prospects in Post-Lisbon Europe « 2011.
67. V. Michel Troper, Véronique Champeil-Desplats et Christophe Grzegorzczak, *Théorie des contraintes juridiques*. LGDJ, 2005.
68. Ibid.
69. V. not. : Olivia Tambou, « Propos libres autour de l'invalidation par la CJUE de la décision Safe Harbor », Dalloz Actualité, 9 octobre 2015 ; Sylvie Peyrou, « Protection des données et relations transatlantiques (suite)...L'arrêt Schrems de la CJUE », GDR-ELSJ, 7 octobre 2015.
70. *Digital Rights Ireland Ltd & Michael Seitlinger e.a.*, préc.. V. Florence Benoit-Rohmer, « Protection des données personnelles ; Note sous Cour de justice de l'Union européenne, grande Chambre, 8 avril 2015, Digital Rights Ireland Ltd contre Minister for Communications, Marine and Natural Resources et autres et Kärnter Landesregierung Seitlinger et autres, affaires jointes numéros C-293/12 et C-594/12 », RTDE 2015, p.168 ; Denys Simon, « La révolution numérique du juge de l'Union : les premiers pas de la cybergénéralité », *Europe* n°7, p.4 ; Marie-Laure Basilien-Gainche, « Une prohibition européenne claire de la surveillance électronique de masse », in *Revue des droits de l'homme*, 14 mai 2014.
71. *Digital Rights Ireland Ltd & Michael Seitlinger e.a.*, préc., §33
72. Ibid., §54 et 55
73. Concl. de l'avocat général Yves Bot sur l'affaire C-362/14, préc., §207.
74. CJUE, 29 janvier 2008, Promusicae, Aff. C-275/06, Rec. p. I-271, § 68
75. CJUE, 18 juin 1991, ERT, C-260/89, Rec. p. I-2925, § 41.
76. *Google Spain SL et Google Inc. c. Agencia Española de Protección de Datos et Mario Costeja González*, préc.
77. CJUE, 23 avril 1986, Les Verts/Parlement, Aff. 294/83, §23; CJUE, 15 mai 1986, Johnston, Aff. 222/84, §18 et 19; CJUE, 15 octobre 1987, Heylens e.a., Aff. 222/86, §14.
78. Ibid.
79. Cour. EDH, Gr. Ch., 4 mai 2000, Rotaru c. Roumanie, req. n°28341/95.

80. Cour. EDH, Gr .Ch., 4 décembre 2008, *S. et Marper c. Royaume Uni*, Req. n° 30562/04 et 30566/04. V., sur cet arrêt : Sylvie Peyrou-Pistouley, « L'affaire *Marper c/ Royaume-Uni* : un arrêt fondateur pour la protection des données dans l'espace de liberté, sécurité, justice de l'Union européenne », *RFDA* 2009, p.94 ; Rocco Bellanova et Paul De Hert, « Le cas *S. et Marper* et les données personnelles : l'horloge de la stigmatisation stoppée par un arrêt européen », *Cultures & Conflits* [En ligne], 76 | hiver 2009, mis en ligne le 03 mai 2011.
81. *Kennedy c. Royaume-Uni*, préc.
82. Cour EDH, 26 mars 1987, *Leander c. Suède* ; Cour EDH, 2 août 1984, *Malone c. Royaume-Uni* ; Cour EDH, 24 avril 1990, *Huvig c. France* ,Cour EDH, 22 juin 2006, *Weber et Saravia c. Allemagne*, no. 54934/00, §§ 4-6 et 78 ; *Kennedy c. Royaume-Uni*, préc.
83. Cour EDH, 24 avril 1990, *Huvig contre France*, Req. n°11105/84, § 34, Cour EDH, 16 février 2000, *Amann c. Suisse*, Req. n° 27798/95, §§ 56-58 ; *Weber et Saravia c. Allemagne*, préc., § 95.
84. *Ibid.*
85. *Ibid.*
86. *Ibid.*
87. Lorna Woods, "Zakharov v Russia: Mass Surveillance and the European Court of Human Rights", *EU Law analysis*, 16 décembre 2015.
88. *Kennedy c. Royaume-Uni*, préc, §159.
89. *Kennedy c. Royaume-Uni*, préc. § 31.
90. Cour EDH, 26 avril 2007, *Dumitru Popescu c. Roumanie*, Req. n° 71525/01, § 71.
91. *Klass et autres contre Allemagne*, préc., §51 ; *Kennedy c. Royaume-Uni*, préc., § 31.
92. *Ibid.*
93. Cour EDH, 10 février 2009, *Iordachi et autres*, req. n° 25198/02, §47.
94. *Szabo c. Hongrie*, préc.
95. V. en ce sens : Sarah St.Vincent, "Did the European Court of Human Rights Just Outlaw "Massive Monitoring of Communications" in Europe "?", *CDT Blog* 13 janvier 2016.
96. V., du côté du Parlement Européen, la Résolution P7_TA-PROV(2014)0230 du 12 mars 2014 *sur le programme de surveillance de la NSA, les organismes de surveillance dans divers États membres et les incidences sur les droits fondamentaux des citoyens européens et sur la coopération transatlantique en matière de justice et d'affaires intérieures* du 2 mars 2014; et plus récemment, les études du Parlement européen sur les risques et opportunités suscités par les mutations numériques et l'émergence de la surveillance de masse : « Mass surveillance, part II – Technology foresight, options for longer term security and privacy improvements » ; « Mass surveillance, part I – Risks and opportunities raised by the current generation of network and applications », décembre 2014.
97. V., publié quelques mois après les révélations Snowden : Arcadio Diaz Terera, « La sécurité nationale et l'accès à l'information », Conseil de l'Europe, CDCJ(2013)13293, Strasbourg, Septembre 2013 ; et, plus récemment, Peter Omtzigt, « Les opérations massives de surveillance en Europe », Conseil de l'Europe, CDCJ(2014), AS/Jur(2015)01, Strasbourg, janvier 2015.
98. Report of the Special Rapporteur to the Human Rights Council on the implications of States' surveillance of communications on the exercise of the human rights to privacy and to freedom of opinion and expression, A/HRC/23/40 , 2013.
99. Commission européenne, "EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield", 2 février 2016.
100. V, pour un historique et une présentation : Paul M. Schwartz and Daniel J. Solove, "Reconciling Personal Information in the United States and the European Union," *California Law Review*, vol. 102, no. 4 (2014).

101. Commission européenne, 6 novembre 2015, « Communication on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C -362/14 (Schrems) », COM(2015) 566 final.

102. Steve Peers, « The party's over: EU data protection law after the Schrems Safe Harbour judgment », EU Law Analysis, 7 octobre 2015.

103. Alexander Bickel. *The Least Dangerous Branch*. Yale University Press, 2nd ed., 1986.

RÉSUMÉS

Le 6 octobre 2015, la Cour de Justice de l'Union Européenne a invalidé la décision 2000/520/CE relative aux transferts de données à caractère personnel vers les États-Unis validant les principes dits de la « sphère de sécurité » ou Safe Harbor qui constituaient auparavant le fondement des transferts de données de l'Union Européenne vers les États-Unis. Dans un contexte d'interaction et de concurrence entre le droit de la Convention Européenne des droits de l'Homme, il est remarquable de noter que la Cour de Strasbourg a, elle aussi, opéré une condamnation stricte de la surveillance de masse dans son arrêt Zakharov de décembre 2015 et son arrêt Szabo de janvier 2016, tout en élargissant le statut de « victime » en matière de surveillance. Les trois arrêts, condamnant la surveillance de masse, apparaissent tout entier tournés vers une exigence commune de prééminence du droit et d'effectivité des recours, ce qui est inédit au regard des positions précédentes de ces juridictions. Cette nouvelle approche ne semble avoir d'autre but que d'instaurer plus aisément un dialogue direct avec les citoyens et d'instaurer une perméabilité des discours juridictionnels et des discours « militants », la révélation de l'existence du programme « Prism » par Edward Snowden jouant, en toile de fond, un rôle prééminent dans le raisonnement mené par les juges de Luxembourg et de Strasbourg. L'on peut indéniablement parler en la matière de l'émergence d'un droit « Post-Snowden », marqué de manière subtile par le développement et la légitimation des techniques de surveillance, mais aussi par la remise en cause croissante des aspects les plus liberticides de celle-ci. A cet égard, si les arrêts commentés sonnent en apparence le glas de la surveillance de masse, ceux-ci semblent également en partie aller une reconnaissance de l'inévitabilité du développement de celle-ci, dont les effets devraient alors être contre-balancés par un contrôle effectif des cours sur les abus d'une surveillance de ce type. La frontière entre les valeurs de liberté et les valeurs de sécurité est ainsi plus que jamais mouvante et incertaine.

AUTEUR

JEAN-PHILIPPE FOEGLE

Doctorant en droit public (CREDOF - Université Paris Ouest Nanterre) et allocataire doctoral (Conseil régional d'Ile de France)