PROTECTION DES DONNÉES PERSONNELLES

SERVICE DE L'EXÉCUTION DES ARRETS DE LA COUR EUROPÉENNE DES DROITS DE L'HOMME
DG1

FICHE THÉMATIQUE

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Septembre 2022

PROTECTION DES DONNÉES PERSONNELLES

Ces résumés sont réalisés sous la seule responsabilité du Service de l'exécution des arrêts de la Cour européenne et n'engagent en aucun cas le Comité des Ministres.

1. PROTECTION DES DONNÉES PERSONNELLES 3

1.1. Collecte et utilisation des données personnelles 3

1.2. Perquisition et saisie de données personnelles, y compris la correspondance 7

1.3. Suivi de la correspondance en prison 10

1.4. Données personnelles relatives à la santé 14

1.5. Accès et effacement ou destruction de données personnelles 16

2. SURVEILLANCE SECRÈTE 19

2.1. Interception de communications et de données personnelles 19

2.2. Surveillance sur le lieu de travail 23

2.3. Surveillance de masse 25

Index des affaires 28

La protection des données à caractère personnel revêt une importance fondamentale pour la jouissance par une personne de son droit au respect de la vie privée et familiale, du domicile et de la correspondance, tel que garanti notamment par l'article 8 de la Convention. Dans sa jurisprudence, la Cour européenne s'est référée au concept de « données à caractère personnel » utilisé dans la Convention STE n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, et a adopté une définition large des données à caractère personnel comme étant « toute information concernant une personne physique identifiée ou identifiable ».

La Cour européenne a également noté que les développements technologiques en matière de « traitement automatique » des données avaient conduit, au cours des dernières décennies, à d'énormes défis pour la protection des données personnelles, en particulier en ce qui concerne les possibilités opérationnelles modernes de surveillance, d'interception des communications et/ou de conservation des données.

La présente fiche fournit des exemples de mesures générales et individuelles signalées par les États dans le cadre de l'exécution des arrêts de la Cour européenne concernant divers aspects de la protection des données à caractère personnel : collecte et utilisation de données à caractère personnel, perquisition et saisie de données à caractère personnel, y compris la correspondance, surveillance de la correspondance en prison, données à caractère personnel relatives à la santé, accès aux données à caractère personnel, effacement et destruction de celles-ci, interception des communications et des données à caractère personnel, surveillance sur le lieu de travail et surveillance de masse.

1. PROTECTION DES DONNÉES PERSONNELLES

1.1. Collecte et utilisation des données personnelles

L'affaire concernait la rétention et la défaillance à restituer au requérant des objets saisis dans le cadre d'une enquête pénale en raison de leur perte par négligence par le Bureau du Procureur (correspondance personnelle et professionnelle, documents comptables, cassettes vidéo contenant des enregistrements de réunions d'affaires et passeport international). En 2000, le Code de procédure pénale a été amendé afin de garantir que tout refus des autorités d'investigation ou de poursuite de restituer les objets saisis soit soumis à un contrôle judiciaire. Une indemnité peut être demandée en vertu de l'article 49 de la loi sur les obligations et les contrats.

BGR / Krasimir Yordanov (50899/99

Arrêt définitif le 15/05/2007

Résolution finale CM/ResDH(2016)306

L'affaire concernait une violation du droit du requérant au respect de sa réputation et de son honneur (en tant que partie intégrante de son droit à la vie privée) par un arrêt interne qui l'a identifié nommément comme ayant harcelé un collègue de travail, alors que l'accusé dans l'affaire ne soit pas lui mais son employeur de la collectivité locale. L'arrêt interne l'avait ainsi stigmatisé et était susceptible d'avoir un impact majeur sur son statut professionnel, son honneur et sa réputation.
En 2019, l'arrêt de la Cour a été analysé par le Conseil général de la magistrature dans un rapport soulignant que les tribunaux internes ont l'obligation de concilier de manière adéquate les droits et intérêts constitutionnels des parties concernées (d'une part, le droit à la protection et à la défense judiciaires, les garanties procédurales liées au principe de transparence et la nécessité de motiver les décisions et résolutions et, d'autre part, le droit à la vie privée et à la protection des données à caractère personnel (exigeant que l'inclusion de données d'identification (ou leur anonymisation) soit motivée au regard de sa finalité juridique et de sa proportionnalité...). Des sessions de formation spécifiques à cet égard ont été organisées à l'Académie de formation judiciaire.

ESP / Vincent Del Campo (25527/13)

Arrêt définitif le 06/11/2018

Bilan d'action DH-DD(2019)1004

L'affaire concernait l'ingérence disproportionnée des autorités dans la vie privée du requérant en raison de la publication dans le Journal officiel, sur la base des dispositions de la loi de 1995 sur la divulgation d'informations, d'informations sur le service du requérant dans le KGB en tant que chauffeur pendant la période 1980-1991. La dernière de ces publications au Journal officiel pour les mêmes motifs a eu lieu en 2009. À la lumière du présent arrêt, le service de sécurité intérieure (KAPO) effectuera désormais le test de proportionnalité avant de divulguer le nom d'une personne et d'autres données.

EST / Soro (22588/08)

Arrêt définitif le 03/12/2015

Résolution finale CM/ResDH(2017)152

Cette affaire concernait un requérant, condamné dans le cadre d'une manifestation, dont le refus de se soumettre à un test ADN et d'être inscrit dans le fichier national informatisé des empreintes génétiques (FNAEG) a entraîné une condamnation pénale. La Cour européenne a souligné qu'aucune suite n'avait été donnée à la décision du Conseil constitutionnel de 2010 exigeant - en ce qui concerne le fichier des empreintes génétiques - une détermination « de la durée de conservation de ces données à caractère personnel en fonction de la finalité du fichier conservé et de la nature et/ou de la gravité des infractions en cause » et a jugé que la réglementation relative à la conservation des profils ADN dans le FNAEG n'offrait pas aux personnes concernées une protection suffisante.

FRA / Aycaguer (8806/12)

Arrêt définitif le 22/09/2017

Résolution finale CM/ResDH(2022)84

Suite à l'arrêt de la Cour, certains tribunaux internes ont adapté leur jurisprudence afin d'éviter la condamnation pénale des personnes refusant de se soumettre à un test ADN en vue de leur inscription au FNAEG. Par la suite, en octobre 2021, le Code de procédure pénale et les dispositions relatives au FNAEG ont été modifiés par décret afin de mettre en œuvre la décision du Conseil constitutionnel de 2010 et l'arrêt de la CEDH. Ainsi, le profil génétique d'une personne condamnée pour l'une des infractions visées à l'article 706-55 du Code de procédure pénale est conservé pendant 25 ans et seulement exceptionnellement pendant 40 ans, pour des faits considérés comme d'une particulière gravité. Ces durées sont fixées à 15 et 25 ans pour les mineurs. Par ailleurs, une loi de mars 2019 permet désormais aux personnes condamnées de demander le retrait anticipé de leur profil génétique du FNAEG.

L'affaire concernait la collecte et la conservation des empreintes digitales du requérant dans la base de données nationale des empreintes digitales (« la FAED ») dans le cadre d'une enquête menée à son encontre concernant un vol de livres, qui s'est terminée par une décision de ne pas intenter de poursuites. Suite à l'arrêt du tribunal concluant à une ingérence disproportionnée dans la vie privée du requérant, ses empreintes digitales ont été effacées de la base de données. En décembre 2015, un décret modifiant le décret FAED de 1987 a été adopté, limitant son application aux crimes et délits graves. Il a également introduit une distinction entre les systèmes de conservation des empreintes digitales des personnes contre lesquelles l'autorité judiciaire a estimé que les chefs d'accusation étaient insuffisants et les autres. En ce qui concerne les personnes qui reçoivent une décision de justice définitive déclarant leur innocence (relaxe ou acquittement), les données seront immédiatement et automatiquement effacées. En cas de renvoi ou de classement pour insuffisance de chefs d'accusation, les données peuvent être effacées à la demande de la personne concernée mais peuvent être conservées pendant trois à dix ans, selon la nature de l'infraction. A l'expiration de ces délais, la suppression des données est automatique.

FRA / M.K. (19522/09)

Arrêt définitif le 18/07/2013

Résolution finaleμ CM/ResDH(2016)310

L'affaire concernait la divulgation non autorisée des relevés téléphoniques du requérant, fournis par l'opérateur national de téléphonie fixe à la partie adverse dans le cadre d'une procédure civile de succession, et leur utilisation par le tribunal interne pour rejeter, en partie, la demande d'exonération des frais de justice du requérant.
Pour prévenir des violations similaires, la loi de 2011 sur la protection des données personnelles a créé une autorité de contrôle du traitement des données personnelles, le Centre national pour la protection des données personnelles, avec le devoir de surveiller le respect de la législation sur la protection des informations, et en particulier, le droit à l'information, l'accès aux données et leur intégrité. Une stratégie nationale de protection des données et un plan d'action pour sa mise en œuvre ont été adoptés pour 2013-2018. Des activités de formation pertinentes pour les juges et autres professionnels du droit ont été organisées par l'Institut national de la justice.

MDA / Savotchko (33074/04)

Arrêt définitif le 28/06/2017

Résolution finale CM/ResDH(2018)130

L'affaire concerne le manquement des tribunaux internes à protéger la vie privée de la requérante en rejetant son action contre un journal, qui avait divulgué son adresse résidentielle dans un article concernant un cambriolage à son domicile, en se fondant sur le fait que la requérante était une personnalité publique et un sujet d'intérêt public.
La violation découlait de l'évaluation erronée par les tribunaux internes des intérêts contradictoires et de la notion d'« intérêt public ». Suite à cet arrêt, la Cour de cassation a modifié sa jurisprudence en conséquence. L'arrêt a été publié et diffusé, et utilisé dans des activités de formation pour les juges nationaux.

TUR / Alkaya (42811/06)

Arrêt définitif le 09/01/2013

Résolution finale CM/ResDH(2016)209

L'affaire concernait la divulgation du nom et de la photographie de la requérante dans des articles de journaux, la présentant comme une kamikaze malgré des enquêtes classées sans suite, ainsi

TUR / Tarman (63903/10)

que l'incapacité subséquente des autorités à protéger sa réputation et le rejet de ses requêtes en dommages et intérêts contre le rédacteur en chef et les journalistes. La violation étant due à une pratique erronée des tribunaux internes, l'arrêt de la Cour européenne a entraîné un changement de jurisprudence, en particulier de la Cour de cassation et de la Cour constitutionnelle.

Arrêt définitif le 21/02/2018

Résolution finale CM/ResDH(2019)215

L'affaire concernait l'ingérence disproportionnée dans la vie privée du requérant en raison de l'obligation de divulguer son appartenance religieuse sur sa carte d'identité.
Pour éviter des violations similaires, un cadre juridique réformé régissant les cartes d'identité a été introduit en 2016. Les nouvelles cartes d'identité contiennent une puce électronique, qui ne peut contenir des informations sur l'appartenance religieuse d'une personne que si celle-ci y consent expressément dans le formulaire de demande. Les informations stockées sur les puces électroniques sont classifiées et le droit d'accès des autorités ne doit être accordé par la loi que dans la mesure où cela est strictement nécessaire à l'exercice de leurs fonctions. En ce qui concerne les registres d'état civil, tout citoyen a le droit de demander, par écrit, d'enregistrer, de modifier ou de laisser en blanc son appartenance religieuse. Ces informations ne sont transférées dans les puces électroniques que si la personne qui demande une nouvelle carte d'identité donne son consentement explicite.

TUR / Sinan Isik (21924/05)

Arrêt définitif le 02/05/2010

Résolution finale CM/ResDH(2018)221

L'affaire concerne la conservation des données personnelles d'un militant pacifiste de longue date (entre autres son nom, son adresse, sa date de naissance et sa présence aux manifestations organisées par un groupe de protestation violent) dans une base de données de la police, en dépit du fait que le requérant n'avait jamais été condamné pour une infraction quelconque et que son risque de criminalité violente était faible. La Cour européenne a estimé que la conservation continue de ces données était disproportionnée en raison de l'insuffisance des garanties permettant leur révision et leur suppression.
Toutes les références et entrées concernant le requérant ont été effacées d'ici 2019. Suite à cet arrêt, la base de données National Common Intelligence Requête (NCIA) a été créée pour remplacer les bases de données antiterroristes individuelles des forces de police, afin d'assurer une approche cohérente de l'examen, de la conservation et de l'élimination de ces informations. Une équipe d'experts détermine si un enregistrement est pertinent et nécessaire, et s'il est proportionné pour que l'enregistrement soit ajouté à la base de données. La base de données NCIA prévoit un examen de tous les enregistrements après 6, 7 ou 10 ans, selon la catégorie des données.
Un groupe de travail sur la gestion des dossiers examine et met à jour les directives concernant la gestion des informations par la police. Suite à une consultation publique, un nouveau Code de pratique pour la gestion des informations et des dossiers de la police et la pratique professionnelle autorisée associée ont été produits. Le Code définit les procédures à appliquer en matière de collecte et de conservation des informations que la police doit suivre lorsqu'elle obtient, gère et utilise des informations dans l'exercice de ses fonctions. Sous réserve de leur ratification par les organes de gouvernance de la police, il est prévu que ces documents soient soumis au ministre de l'Intérieur pour approbation finale en 2022. Un calendrier national de conservation, fournissant une liste définitive des périodes de conservation pour toutes les informations de la police, a également été publié.

UK. / Catt (43514/15)

Arrêt définitif le 24/10/2019

Plan d'action DH-DD(2019)1248

Règle 8.2a Communication des autorités (20/12/2021)

L'affaire concernait la conservation indéfinie des données à caractère personnel du requérant (profil ADN, empreintes digitales et photographie) prises dans le cadre d'une condamnation passée en Irlande du Nord pour une infraction de conduite sous l'influence excessive de l'alcool. La Cour européenne a estimé que la nature indiscriminée des pouvoirs de rétention, associée à l'absence de garanties suffisantes, dépassait la marge d'appréciation acceptable de l'État à cet égard.

UK. / Gaughran (45245/15)

Arrêt définitif le 13/06/2020

Plan d'action DH-DD(2021)202

En 2018, la loi sur la protection des données (*Data Protection Act (DPA)*) a introduit des examens périodiques de la conservation des données personnelles, y compris les données biométriques, à des fins d'application de la loi. Elle prévoit également une surveillance par le commissaire à l'information. La DPA s'applique à toutes les régions du Royaume-Uni. La législation spécialisée dans les juridictions décentralisées reste la même qu'au moment où la Cour européenne a examiné les griefs du requérant, à l'exception de l'Écosse où la *Biometrics Commissioner Act 2020* permet au commissaire de fixer des périodes de conservation dans son Code de pratique.

UK. / M.M. (24029/07)

Arrêt définitif le 29/04/2013

Résolution finale CM/ResDH(2015)221

L'affaire concernait l'ingérence illégale dans la vie privée du requérant en raison de la conservation et de la divulgation indéfinies de données concernant un avertissement de la police pour enlèvement d'enfant reçu par le requérant à la suite d'un conflit familial. En outre, le tribunal européen a constaté l'insuffisance de garanties dans le système pour assurer que de telles données privées ne soient pas divulguées, en particulier, à des employeurs potentiels.
En Irlande du Nord, en Angleterre et au Pays de Galles, des modifications statutaires ont été introduites pour mettre en œuvre l'arrêt. Les détails relatifs au requérant ont été supprimés de la base de données des antécédents criminels de l'Irlande du Nord. En Angleterre et au Pays de Galles, des modifications statutaires de 2013 ont introduit un mécanisme de filtrage afin que les avertissements et condamnations anciens et mineurs ne soient plus automatiquement divulgués sur un extrait du casier judiciaire. La divulgation n'est effectuée qu'après avoir pris en compte la gravité et l'ancienneté de l'infraction, l'âge du contrevenant et le nombre d'infractions commises. D'autres modifications statutaires sont entrées en vigueur, permettant aux individus de s'adresser à un organisme de contrôle indépendant.
Des modifications législatives similaires sont entrées en vigueur en Irlande du Nord en avril 2014. La loi sur la justice (Irlande du Nord) de 2015 a modifié l'ordonnance de 1989 sur la police et les preuves criminelles (Irlande du Nord) afin de créer un pouvoir légal pour l'enregistrement des avertissements et autres dispositions alternatives dans la base de données des antécédents criminels de l'Irlande du Nord.
Le régime écossais ne permet pas la divulgation automatique des « alternatives aux poursuites » (équivalentes aux cautions en Angleterre et au Pays de Galles), qui sont retirées du système après une période de deux ou trois ans. Pour certaines infractions sexuelles et violentes graves, les informations peuvent être conservées jusqu'à deux ans supplémentaires après une requête adressée à un tribunal par le chef de la police.

UK. / Peck (44647/98)

Arrêt définitif le 28/04/2003

Résolution finale CM/ResDH(2011)177

L'affaire concernait la divulgation dans les médias par un conseil local des photographies d'un individu prises par une caméra de vidéosurveillance installée dans une rue publique, sans consentement ni garanties suffisantes, et l'absence de recours effectif à cet égard. Pour prévenir des violations similaires, des dispositions spécifiques sont contenues dans la loi sur la protection des données de 1998 (DPA) et le Code de pratique de la vidéosurveillance (CCTV) 2008 du commissaire à l'information. La DPA fournit la base légale du contrôle juridique systémique de la vidéosurveillance des zones publiques, en fixant des normes juridiquement exécutoires pour la collecte et le traitement des images relatives aux individus. Le commissaire à l'information a le pouvoir de faire respecter la DPA, y compris d'imposer des sanctions pécuniaires en cas de violations graves. Le Code de pratique de la vidéosurveillance (CCTV) de 2008 a été révisé pour tenir compte de l'évolution de la loi, de la technologie, de l'utilisation de la vidéosurveillance et des lacunes identifiées par la Cour européenne. Il exige la justification systématique de l'utilisation de la vidéosurveillance, l'amélioration de la qualité des images et impose des restrictions sur la surveillance et l'enregistrement des conversations dans les espaces publics.

UK. / S. et Marper (30562/04)

L'affaire concernait l'ingérence injustifiée dans le droit des requérants mineurs au respect de leur vie privée en raison de la conservation indéfinie d'échantillons de sang, d'empreintes digitales et

de profils ADN prélevés dans le cadre de leur arrestation pour des infractions pour lesquelles ils n'ont finalement pas été condamnés.
Suite à cet arrêt, les empreintes digitales, les échantillons et profils ADN des requérants ont été détruits.
En 2012, la loi sur la protection des libertés a créé un nouveau régime pour la conservation des échantillons (ADN et empreintes digitales) et des données biométriques. En particulier, elle a introduit un délai de trois ans pour la conservation des empreintes digitales et des profils ADN pour les personnes appréhendées mais non condamnées pour une infraction grave, avec une prolongation possible et unique de deux ans sur demande de la police auprès des tribunaux nationaux. En outre, un commissaire à la biométrie a été nommé, dont le rôle est, entre autres, de surveiller la conservation et l'utilisation du matériel biométrique.
La loi de 2013 sur la justice pénale (Irlande du Nord) contenait des dispositions similaires à celles de la loi sur la protection des libertés. À la suite d'une erreur de rédaction initiale, un amendement a été apporté par l'Assemblée d'Irlande du Nord à la loi sur la justice (Irlande du Nord) de 2015. Cependant, le nouveau régime de conservation des échantillons et des données biométriques (ADN et empreintes digitales) en Irlande du Nord n'a toujours pas commencé, en raison des inquiétudes concernant le fait que les enquêtes futures sur les décès liés aux troubles en Irlande du Nord pourraient être compromises, si le matériel biométrique lié à ces affaires était détruit. En mars 2020, le service de police d'Irlande du Nord a décidé de suspendre la suppression des données biométriques sur une base non statutaire et d'attendre l'entrée en vigueur complète de cette loi.

Arrêt définitif le 04/12/2008

Rapport d'action DH-DD(2015)836

Règle 8.2a Communication des autorités (09/04/2021)

1.2. Perquisition et saisie de données personnelles, y compris la correspondance

L'affaire concernait une inspection dans les locaux de la société requérante dans le cadre d'une procédure administrative sans autorisation préalable d'un juge et sans contrôle effectif *a posteriori* de la décision. La société requérante s'est vu infliger par la suite une amende pour avoir refusé d'autoriser un examen approfondi de ses données alors qu'elle avait accordé l'accès à certaines lettres de ses représentants.
Afin de prévenir des violations similaires, le Code de justice administrative a été modifié en 2012 pour introduire la possibilité d'une action devant les tribunaux administratifs contre des interférences déjà classées. En outre, en février 2016, la Cour administrative suprême a modifié sa jurisprudence en confirmant explicitement que de telles actions peuvent également être utilisées pour contester les inspections sur site. Enfin, la loi de 2001 sur la protection de la concurrence a également été modifiée en 2016 et mise en conformité avec cette position.

CZE / Delta Pekárny a.s. (97/11)

Arrêt définitif le 02/01/2015

***Résolution finale* CM/ResDH(2017)299**

L'affaire concernait la saisie par la police et l'accès de cette dernière à l'ordinateur du requérant au motif qu'il contenait du matériel pédopornographique, en contournant l'exigence normale d'une autorisation judiciaire préalable, alors qu'en fait l'ordinateur en question était déjà entre les mains de la police et qu'une autorisation préalable aurait pu être obtenue rapidement sans entraver les enquêtes de police. En 2008, le requérant a été condamné à quatre ans d'emprisonnement pour possession et circulation d'images pornographiques de mineurs. En 2015, la loi de procédure pénale a été modifiée pour renforcer les garanties procédurales, en introduisant le recours en révision des arrêts pénaux définitifs, qui avaient été contestés dans des arrêts de la CEDH. L'arrêt a été diffusé auprès des autorités concernées.

ESP / Trabajo Rueda (32600/12)

Arrêt définitif le 30/08/2017

Résolution finale CM/ResDH(2019)50

L'affaire concernait l'impossibilité pour les requérants de contester la légalité de perquisitions et de saisies domiciliaires effectuées dans le cadre d'une procédure fiscale en vertu du Code de procédure fiscale. En fin de compte, aucun des requérants n'a été poursuivi par l'administration fiscale à la suite des procédures en cause. En 2008, le Code de procédure fiscale a été modifié, ouvrant la possibilité de faire appel d'une ordonnance de perquisition devant le premier président de la cour d'appel, compétent pour examiner les faits et le droit. L'amendement prévoit également la compétence de ce dernier pour examiner les recours formés à l'encontre du déroulement des opérations de perquisition et de saisie.

FRA / Ravon et autres (18497/03)

Arrêt définitif le 21/05/2008

Résolution finale CM/ResDH(2012)28

L'affaire concernait la perquisition de locaux résidentiels et commerciaux, et la saisie de documents en rapport avec une infraction au Code de la route commise par un tiers intervenant sans commission rogatoire suffisamment motivée. Dans un arrêt de principe de 1997, la Cour constitutionnelle fédérale a reconnu le droit du requérant à ce que la légalité de l'ordonnance de perquisition et de saisie soit examinée rétrospectivement.
L'arrêt de la Cour a été diffusé à tous les tribunaux et autorités judiciaires concernés.

GER / Buck (41604/98)

Arrêt définitif le 28/07/2005

Résolution finale CM/ResDH(2007)80

L'affaire concernait la saisie des deux ordinateurs du requérant et de centaines de documents en son absence, sur la base d'un mandat rédigé en termes trop généraux en raison de l'interprétation erronée de la loi sur les opérations de perquisition et de saisie, dans le cadre d'enquêtes pénales préliminaires. La directive européenne 2016/680 sur le traitement des données à caractère personnel à des fins de prévention, de recherche, de détection ou de poursuite d'infractions pénales (transposée en droit grec) vise à garantir un niveau élevé de protection, tout en veillant à ce que les enquêtes et les poursuites pénales ne soient pas entravées. La directive s'applique au traitement transfrontalier et interne des données à caractère personnel. Elle établit également une autorité de contrôle à laquelle toutes les personnes qui estiment que leurs données personnelles ont été violées peuvent adresser leurs griefs.

GRC / Groupe Modestou (51693/13)

Arrêt définitif le 18/09/2017

Rapport d'action DH-DD(2019)1096

L'affaire concernait la perquisition illégale du cabinet d'un avocat par la police en son absence et la saisie sans discernement de tous les documents trouvés concernant un de ses clients soupçonné d'être impliqué dans des activités financières illégales. Suite à l'arrêt de la Cour, les documents relatifs à la procédure pénale ont été exclus des preuves par le tribunal interne et les documents saisis ont été restitués à la requérante. La violation ayant résulté d'une application erronée de la loi existante, l'arrêt a été diffusé auprès des autorités internes concernées.

HUN / Turan (33068/05)

Arrêt finalisé le 06/10/2010

Résolution finale CM/ResDH(2018)381

L'affaire concernait l'absence de garanties adéquates et effectives dans le contrôle de la légalité et du champ de la perquisition de l'appartement du requérant et de la saisie de ses effets personnels, y compris un ordinateur et un disque dur, dans le cadre d'une enquête de la police secrète sur une allégation de vente sans licence de médicaments pour le traitement du VIH, de l'hépatite et du cancer via Internet. Par la suite, le bureau du procureur et les tribunaux administratifs n'ont pas procédé à un examen *ex post* adéquat et efficace des actions contestées. Pour améliorer le contrôle des perquisitions et des saisies par les procureurs, le Procureur général a publié un décret en 2010 afin d'intensifier le contrôle des procureurs dans les procédures concernant des infractions présumées commises par des agents de l'État, qui sont désormais examinées en priorité. Depuis 2012, la qualité du contrôle du ministère public fait l'objet d'une évaluation continue. Des exemples de jurisprudence des tribunaux administratifs concernant des actions de fonctionnaires de police de l'État ont été soumis, dans lesquels les tribunaux ont reconnu les violations des droits de l'homme par la police et ont accordé une indemnité monétaire.

LVA / Boze (40927/05)

Arrêt définitif le 13/11/2017

Résolution finale CM/ResDH(2019)299

L'affaire concernait une perquisition menée par la police au domicile du requérant dans le cadre d'une procédure de contravention à l'encontre d'un tiers, sans mandat rogatoire ni autorisation judiciaire, en violation de la loi interne. Pour prévenir des violations similaires, le Code des infractions mineures de 2009 a prévu des garanties supplémentaires pour la conduite de perquisitions dans les affaires d'infractions mineures, en exigeant l'affirmation motivée d'un agent de l'État sur l'infraction mineure et l'autorisation préalable d'un tribunal. En cas d'infraction mineure flagrante, une perquisition peut exceptionnellement être effectuée sans l'autorisation préalable d'un tribunal, dans des conditions spécifiques. Le Code de procédure pénale prévoit que, dans le cadre d'une procédure pénale, la perquisition d'un domicile ne peut être effectuée qu'avec l'autorisation préalable du propriétaire, du détenteur du titre ou d'un membre majeur de la famille.

MDA / Bostan (52507/09)

Arrêt définitif le 08/03/2021

Résolution finale CM/ResDH(2021)291

L'affaire concernait une ingérence illégale due à l'utilisation d'une procédure d'urgence pour confisquer la correspondance postale du requérant dans le cadre d'une procédure pénale sans autorisation judiciaire.
La procédure contestée a été modifiée dans le Code de procédure pénale de 2014. Les saisies et perquisitions des envois postaux sont désormais soumises à une autorisation judiciaire.

ROM / Dragos Ioan Rusu (22767/08)

Arrêt définitif le 31/01/2018

Résolution finale CM/ResDH(2019)225

L'affaire concernait une perquisition de la police dans l'appartement du requérant et le prélèvement d'un échantillon d'ADN au cours d'une enquête sur un meurtre. Le tribunal a estimé que le prélèvement de l'échantillon de salive ADN n'avait pas été « conforme à la loi » au sens de l'article 8. En particulier, l'ordonnance autorisant la police à prélever un échantillon de salive du requérant ne se référait à aucune disposition légale spécifique, le Code de procédure pénale ne contenant aucune référence au prélèvement d'échantillons d'ADN. En outre, les autorités n'avaient pas établi de procès-verbal officiel de la procédure.
Le Code de procédure pénale a été révisé en 2011. Il contient des garanties supplémentaires concernant les prélèvements buccaux d'ADN et l'obligation que seul un expert puisse effectuer la procédure.

SER / Dragan Petrovic (75229/10)

Arrêt définitif le 14/08/2020

Plan d'action DH-DD(2021)328

L'affaire concernait des irrégularités dans la conduite de perquisitions et de saisies au domicile du requérant et dans son étude notariale, ainsi que la divulgation d'informations psychiatriques confidentielles dans le cadre d'une procédure en diffamation, en raison de la mauvaise application des dispositions légales pertinentes par les tribunaux internes. Par conséquent, des activités de formation et des séminaires sur les exigences de la CEDH lors de la conduite d'inspections, de perquisitions ou d'enquêtes secrètes ont été organisés pour les autorités chargées de l'application de la loi et pour les bureaux des procureurs régionaux. En ce qui concerne la possibilité de contester la légalité d'un ordre de perquisition, en vertu du Code de procédure pénale de 2012, les pièces à conviction obtenues à la suite d'une perquisition illégale deviennent irrecevables. Par ailleurs, par une décision de 2019, la Cour suprême a introduit la possibilité de contester la conformité d'une perquisition/opération d'enquête devant les tribunaux administratifs.

UKR / Panteleyenko (11901/02)

Arrêt définitif le 12/02/2007

Résolution finale CM/ResDH(2021)137

Ces affaires concernaient diverses irrégularités liées à l'interception de la correspondance et aux perquisitions dans les locaux des avocats. En réponse, les autorités ont mis en place des mécanismes de contrôle judiciaire étendus et des délais pour l'interception des correspondance et communications ont été introduits. Le Code de procédure pénale de 2012 a fourni des garanties concernant les perquisitions de locaux et la saisie de documents et d'autres biens, allant d'une définition étendue du domicile (couvrant également les locaux non résidentiels) à

UKR / Voskoboynikov (33015/06)

Arrêt définitif le 05/10/2017

UKR / Golovan (41716/06)

l'exigence d'autorisations judiciaires préalables pour les perquisitions ainsi qu'à l'obligation de rejeter les demandes infondées des procureurs ou des enquêteurs. Les perquisitions sans autorisation judiciaire préalable ne sont autorisées qu'en cas d'urgence et/ou de poursuite d'un criminel en fuite. Une violation de ces règles entraîne l'irrecevabilité des pièces à conviction recueillies. Des garanties supplémentaires, introduites en 2017, incluent l'enregistrement audio et vidéo des perquisitions, ainsi que la présence d'avocats et de témoins non professionnels. Les perquisitions dans les locaux des avocats nécessitent une notification préalable du conseil régional des barreaux et la présence de son représentant. La responsabilité pénale est prévue pour les entrées et perquisitions illégales. La décision d'un juge d'instruction ordonnant la saisie de biens est susceptible d'appel. En outre, une demande d'annulation de la saisie peut être déposée auprès d'un juge d'instruction ou d'un tribunal.

Arrêt définitif le 05/10/2012

UKR / Volokhy (23543/02)

Arrêt définitif le 02/02/2007

UKR / Les affaires du groupe Koval et autres (22429/05)

Résolution finale CM/ResDH(2021)48

1.3. Suivi de la correspondance en prison

L'affaire concernait la surveillance injustifiée par l'administration pénitentiaire du formulaire de requête du requérant envoyé à la Commission européenne des droits de l'homme. En 1998, la loi sur l'exécution des peines a prévu que les correspondances adressées aux institutions des droits de l'homme de l'ONU et du Conseil de l'Europe ne sont pas soumises au contrôle de l'administration.

BGR / Mironov (30381/96)

Arrêt définitif le 12/04/1999

Résolution finale CM/ResDH(2004)15

La violation constatée dans cette affaire concernait la surveillance systématique injustifiée de la correspondance en prison, y compris la correspondance avec les avocats. En 2009, la loi sur l'exécution des peines et la détention provisoire est entrée en vigueur, réglementant le droit à la correspondance et à l'utilisation du téléphone des prisonniers. Le contrôle de la correspondance des prisonniers ne concerne que le contenu matériel et non le contenu écrit de la lettre. Dans un arrêt de 2013, la Cour suprême de cassation a estimé que les demandes d'indemnité introduites par des détenus alléguant une imputation de leur droit à la correspondance devaient être examinées par les tribunaux administratifs en vertu de la loi de 1988 sur la responsabilité de l'État et des municipalités en cas de dommages.

BGR / Groupe Petrov (15197/02)

Arrêt définitif le 22/08/2008

Résolution finale CM/ResDH(2014)258

L'affaire concernait l'ingérence illégale dans la vie privée d'un détenu en raison de la surveillance de sa correspondance adressée au Médiateur et au Procureur général ainsi qu'au tribunal, pendant son isolement cellulaire. En juillet 2018, le Parlement a modifié le Règlement pénitentiaire en ce qui concerne la correspondance et les communications téléphoniques des détenus ainsi que l'isolement cellulaire en tant que sanction disciplinaire ou à des fins autres qu'une sanction disciplinaire formelle.

CYP / Onoufriou (24407/04)

Arrêt définitif le 07/04/2010

Résolution finale CM/ResDH(2019)86

L'affaire concernait une ingérence disproportionnée due à l'ouverture de la correspondance du requérant par les autorités pénitentiaires.
En 2000, la loi sur l'emprisonnement a établi qu'un agent pénitentiaire peut ouvrir les lettres envoyées par ou à un détenu en présence du destinataire, à l'exception des lettres adressées à son avocat, à un procureur ou à un tribunal (y compris la Cour européenne, le Chancelier juridique et le ministère de la Justice).

EST / Slavgorodski (37043/97)

Arrêt définitif le 12/12/2000

Résolution finale CM/ResDH(2001)101

L'affaire concerne les mauvaises conditions de détention dans la prison pour hommes de Korydallos et l'ingérence dans la correspondance.
En 2000, le Code de procédure pénale relatif à l'application des peines a été modifié afin de supprimer la distinction entre la correspondance entre les accusés et les avocats qui les avaient assistés dans la procédure pour laquelle ils étaient détenus, qui n'était pas soumise à un contrôle, et la correspondance entre les accusés et les avocats qui ne les avaient pas assistés dans la procédure, qui était soumise à un contrôle. En outre, un mémorandum a été envoyé aux directeurs de prison précisant que la correspondance des détenus avec la Commission des droits de l'homme ou la Cour européenne ne devait pas être ouverte.

FRA / Slimane-Kaid (27019/95)

Arrêt définitif le 12/04/1999

Résolution finale CM/ResDH(2007)50

L'affaire concernait les mauvaises conditions de détention dans la prison pour hommes de Korydallos et l'ingérence dans la correspondance des prisonniers. Le Code pénitentiaire de 1999 a introduit des garanties suffisantes pour la protection de la correspondance des détenus, interdisant explicitement tout contrôle de la correspondance et de la forme de communication des détenus, sauf si cela est nécessaire pour des raisons de sécurité nationale ou lié à des infractions particulièrement graves. Lorsqu'une restriction est imposée à la correspondance ou aux communications, le détenu peut faire appel auprès du juge compétent en vertu de la loi de 1994 sur la liberté de la correspondance et de la communication.

GRC / Peers (28524/95)

Arrêt définitif le 19/04/2001

Résolution finale CM/ResDH(2009)127

Ces affaires concernaient le manque de clarté de la législation interne sur la surveillance de la correspondance des détenus, laissant aux autorités une trop grande marge de manœuvre, notamment en ce qui concerne la durée des mesures de surveillance et les raisons justifiant ces mesures, autorisant la surveillance de la correspondance avec les organes de la Convention européenne des droits de l'homme et ne prévoyant aucun recours effectif contre les décisions ordonnant la surveillance de la correspondance. Afin de prévenir toute ingérence arbitraire ou non-conforme à la loi de 1975 sur l'administration des prisons dans la correspondance des détenus, une réforme législative de l'administration pénitentiaire a été adoptée en 2004, définissant des motifs clairs de restriction de la correspondance des détenus et des critères pour la durée de la mesure. Le contrôle judiciaire de la décision respective est devenu disponible en principe. Toutefois, l'efficacité de ce contrôle judiciaire a été contestée, en particulier en ce qui concerne la durée de ces procédures (voir Résolution intérimaire (2005)56 dans le groupe *Messina n° 2*).
Avant cette réforme, en 1999, des circulaires du ministère de la Justice avaient interdit en pratique la censure de la correspondance envoyée par les détenus aux organes de la Convention.

ITA / Calogero Diana (15211/89)

Arrêt définitif le 15/11/1996

Résolution finale CM/ResDH(2005)55

ITA / Labita (26772/95)

Arrêt définitif le 06/04/2000

Résolution finale CM/ResDH(2009)83

L'affaire concernait un traitement inhumain en ce qui concerne une fouille corporelle et les conditions de détention à la prison de Pravieniskes, y compris la surpopulation ; une ingérence illégale due à la surveillance et à la censure des lettres du requérant en prison, y compris les lettres adressées aux organes de la CEDH.
Selon les dispositions du Code d'exécution des peines de 2003, le contrôle et la censure de la correspondance des détenus nécessitent l'autorisation du procureur ou du chef d'établissement pénitentiaire, ou une décision judiciaire. Le Code détermine également les affaires dans lesquelles le contrôle de la correspondance des détenus ne peut être autorisé, qui incluent la correspondance avec les organes de la Convention européenne des droits de l'homme.

LIT / Valasinas (44558/98)

Arrêt final le 24/10/2001

Résolution finale CM/ResDH(2004)41

L'affaire concernait le droit à la correspondance des prisonniers en détention provisoire. Selon l'amendement de 2005 de la loi sur la procédure pénale, leur correspondance ne peut être surveillée que dans le cadre d'une enquête sur des crimes graves ou extrêmement graves et seulement pour une période maximale de 30 jours.

LVA / Lavents (58442/00)

Arrêt définitif le 28/02/2003

	Résolution finale CM/ResDH(2009)131
L'affaire concernait une ingérence injustifiée due au contrôle de la correspondance d'un détenu avec la Commission européenne des droits de l'homme par les autorités pénitentiaires des Antilles néerlandaises, une ingérence dans sa correspondance avec son avocat et un ancien détenu et l'absence de recours effectif. Afin de prévenir toute ingérence injustifiée dans le droit des détenus à la correspondance avec la Commission européenne des droits de l'homme, le règlement du système pénitentiaire des Antilles néerlandaises a été modifié et le Règlement général des prisons adopté en 1999 prévoit que la correspondance avec les destinataires habilités à entendre les griefs des détenus ou les affaires faisant suite à une plainte ne doit pas être surveillée et ne peut être ouverte sans le consentement écrit du détenu. La disposition générale interdisant toute correspondance avec les anciens détenus a également été levée.	***NLD / A.B. (37328/97)*** ***Arrêt définitif le 29/04/2002*** **Résolution finale CM/ResDH(2010)103**
Ces affaires concernaient le contrôle de la correspondance en détention provisoire et le refus des visites familiales et, dans certains cas, le manque de garanties procédurales et la durée excessive de la détention provisoire. En ce qui concerne le contrôle et la censure de la correspondance des détenus en détention provisoire, le Code d'exécution des peines pénales de 1998 a été modifié en 2003 et 2012, prévoyant que la correspondance avec le médiateur et les organismes internationaux de protection des droits de l'homme doit être envoyée directement aux destinataires sans censure. Cette règle s'applique également à la correspondance avec les autorités d'enquête, les autorités judiciaires, les autres organes de l'État et les organes des municipalités. La correspondance entre les personnes détenues en détention provisoire et leurs avocats n'est, en règle générale, pas soumise à la censure. Exceptionnellement, uniquement pendant l'enquête et pour une période n'excédant pas 14 jours à compter du jour de l'arrestation, un procureur peut, dans certaines situations, se réserver le droit de surveiller la correspondance entre le suspect et son avocat. En outre, les personnes qui invoquent l'imputation d'une violation de leur droit au respect de leur correspondance peuvent demander une indemnité en vertu du Code civil.	***POL / Groupe Klamecki n° 2 (31583/96)*** ***Arrêt définitif le 03/07/2003*** **Résolution finale CM/ResDH(2013)228**
L'affaire concerne la surveillance de la correspondance privée et privilégiée, notamment avec l'avocat, par les autorités pénitentiaires en 2008-2009. Les autorités ont pris des mesures législatives, en particulier, en 2012, l'article 91 § 3 du Code d'exécution des peines a été modifié, prévoyant que la correspondance entre un détenu et son avocat ne peut être censurée, sauf s'il existe des informations fiables sur la planification ou la perpétration d'un crime. L'article 15 § 4 prévoit en outre que la correspondance avec les organismes interétatiques de protection des droits de l'homme ne peut être censurée. En 2011, le Service pénitentiaire fédéral a introduit un « Guide à l'intention de son personnel », qui contient une exigence selon laquelle la censure doit être interdite non seulement pour la correspondance des détenus avec leur avocat, mais aussi avec leur représentant devant la Cour européenne, ainsi que d'autres exigences. L'arrêt a été traduit et diffusé auprès des autorités compétentes.	***RUS / Boris Popov (23284/04)*** ***Arrêt définitif le 28/01/2011*** **Bilan d'action DH-DD(2017)924**
Ce groupe d'affaires concerne une ingérence injustifiée des autorités pénitentiaires dans le droit à la correspondance des détenus. Les mesures d'interception et de censure concernées ont été décidées par la commission disciplinaire de la prison et supervisées par le procureur général, et non par un tribunal indépendant, sur la base d'un cadre réglementaire non spécifié. La loi de 2005 sur l'exécution des peines et des mesures préventives et la directive de 2020 sur la gestion des prisons et l'exécution des peines et des mesures préventives visent à apporter suffisamment de clarté sur le droit de contrôler la correspondance des détenus. La	***TUR / Groupe Tamer (6289/02)*** ***Arrêt définitif le 05/03/2007*** **Bilan d'action DH-DD(2021)940**

correspondance entre les détenus et leur avocat et les autorités officielles n'est pas soumise à inspection, sauf pour les détenus condamnés pour des crimes liés au terrorisme ou organisés ou dans des affaires exceptionnelles, si les autorités ont des raisons de croire qu'un abus de privilège a eu lieu et que le contenu de la lettre menace la sécurité de l'établissement ou d'autres personnes ou est autrement illégal.
Le reste de la correspondance générale est inspecté par la commission de lecture de l'administration pénitentiaire et est transmis à la commission disciplinaire, qui peut décider de le conserver, s'il représente une menace pour l'ordre et la sécurité dans la prison, désigne des fonctionnaires en service comme cibles, permet la communication avec une organisation terroriste ou criminelle, contient des informations fausses ou trompeuses susceptibles de semer la panique chez des individus ou des institutions ou contient des menaces ou des insultes. Le détenu peut faire appel de cette décision auprès du tribunal d'exécution, qui doit statuer dans les sept jours. Un autre appel peut être introduit auprès de la cour d'assises.

L'affaire concernait la surveillance injustifiée par les autorités pénitentiaires de la correspondance médicale entre un prisonnier condamné détenu dans une prison de haute sécurité et son médecin spécialiste externe. L'instruction de l'administration pénitentiaire sur les communications avec les détenus a été modifiée en 2011 pour stipuler que : « La correspondance entre un détenu et un médecin agréé doit être traitée de manière confidentielle, mais uniquement dans la mesure où le médecin agréé agit à titre professionnel et où la correspondance est directement liée au traitement du détenu ». En ce qui concerne l'Angleterre et le Pays de Galles, un instrument statutaire de 2010 a modifié les règlements pertinents pour prévoir qu'un détenu peut correspondre de manière confidentielle avec un médecin agréé qui a traité le détenu pour une affection mettant sa vie en danger, et cette correspondance ne peut être ouverte, lue ou arrêtée que si le chef d'établissement pénitentiaire a des « motifs raisonnables » de croire que le contenu n'est pas lié au traitement de cette affection. L'administration pénitentiaire écossaise a adopté une disposition similaire dans la règle 58 des *Prisons and Young Offenders Institutions (Scotland) Rules 2011*, qui est conçue pour être cohérente avec la décision dans cette affaire. L'administration pénitentiaire d'Irlande du Nord a publié une instruction à l'intention des gouverneurs en 2012, modifiant le règlement de l'administration pénitentiaire d'Irlande du Nord. Si un détenu devait développer une maladie potentiellement mortelle pendant son séjour en prison, il n'aurait pas besoin de correspondre avec un consultant car il recevrait des soins sur place de la part des professionnels de la santé. Il y aurait un devoir de diligence de la part de l'équipe de soins de santé de la prison de prendre contact avec le prestataire de soins de santé externe du prisonnier et tout contact de ce type serait couvert par les procédures médicales de confiance déjà en place.	***UK. / Szuluk (36936/05)*** ***Arrêt définitif le 02/09/2009*** **Résolution finale CM/ResDH(2013)88**
L'affaire concernait l'interception et l'ouverture imprévisibles de la correspondance de deux résidents d'une colonie pénitentiaire (qui y travaillaient mais ne purgeaient pas de peine) par l'administration pénitentiaire respective. La violation découlait d'une faute administrative de l'établissement pénitentiaire concerné et d'une mauvaise interprétation de la loi par les tribunaux nationaux dans les circonstances spécifiques de cette affaire. L'instruction du ministère de la Justice de 2013 « Sur l'organisation de la correspondance des personnes détenues dans les établissements pénitentiaires et dans les maisons de correction » a été publiée et est donc accessible au public. Des sessions de formation pour les juges et les candidats aux fonctions judiciaires ont été organisées sur la jurisprudence de la CEDH, y compris le présent arrêt, qui a été traduit, publié et diffusé à toutes les autorités concernées.	***UKR / Mikhaylyuk et Petrov (11932/02)*** ***Arrêt définitif le 10/03/2010*** **Résolution finale CM/ResDH(2018)40**

1.4. Données personnelles relatives à la santé

L'affaire concernait la divulgation d'informations sur l'état de santé de la requérante dans le cadre d'une procédure pénale contre son mari, en particulier, la divulgation de son identité et de ses données médicales dans l'arrêt de la Cour d'appel et les décisions de limiter la confidentialité du dossier du procès à une période de dix ans. Suite au présent arrêt, le Chancelier de Justice a demandé la révision de la décision contestée en application du Code de procédure judiciaire afin de remédier à la situation individuelle. En 1998, la Cour suprême a estimé que le tribunal d'appel - en vertu de la loi sur la publicité des débats judiciaires - avait fait une application erronée de la loi et a prolongé la période pendant laquelle les dossiers de procès doivent rester confidentiels de dix à quarante ans.

FIN / Z. (22009/93)

Arrêt définitif le 25/02/1997

Résolution finale CM/ResDH(99)24

L'affaire concernait l'ingérence injustifiée dans la vie privée en raison de la collecte de données médicales personnelles par un organisme d'État (MAKKEDI) dans le cadre d'une enquête administrative concernant les soins de santé du requérant sur la base de dispositions légales manquant de précision et de protection juridique adéquate contre l'arbitraire.
En 2007, la MADEKKI a été intégrée à l'Inspection de la santé. Concernant la protection des données des patients, la loi de 2009 sur les droits des patients prévoit que ces données ne peuvent être utilisées qu'avec le consentement écrit du patient ou dans les cas prévus par cette loi. La loi énumère les institutions publiques de santé, dont l'Inspection de la santé, qui peuvent recevoir, collecter et utiliser les données des patients. L'Inspection de la santé est autorisée à collecter les données des patients pour assurer la supervision du secteur des soins de santé. L'éventail des fonctions de supervision est défini dans son statut, approuvé par le Cabinet des ministres en 2008. La procédure de collecte des données des patients est établie dans le règlement intérieur de l'Inspection de la santé de 2013. Ces règles prévoient que, dans le cas où une enquête est ouverte par l'Inspection de la santé, un expert doit évaluer le champ d'application des informations nécessaires et déterminer la durée de traitement des données.

LVA / L.H. (52019/07)

Arrêt définitif le 29/07/2014

Résolution finale CM/ResDH(2017)64

L'affaire concernait la divulgation de la séropositivité du requérant dans un certificat l'exemptant de service militaire délivré en 2011. Afin de prévenir des violations similaires, en 2012, à la demande du Médiateur, le tribunal constitutionnel a déclaré inconstitutionnelle la décision gouvernementale de 2005 exigeant que le code de référence de la maladie spécifique des normes médicales soit indiqué dans le certificat d'exemption. En 2013, le Gouvernement a remplacé sa décision en conséquence. Au cours de la période 2016-2019, plus de 240 juges et procureurs ont participé à des activités de formation de l'Institut national de la justice sur les questions liées à l'article 8, notamment sur la protection des données.

MDA / P.T. (1122/12)

Arrêt définitif le 26/08/2020

Résolution finale CM/ResDH(2021)120

L'affaire concernait la divulgation d'informations de nature médicale par un établissement médical à l'employeur d'une personne, y compris des détails sensibles sur sa grossesse, son état de santé et les traitements reçus, malgré une interdiction explicite de divulguer de telles informations dans la législation interne.
En 2012, la loi sur la protection des données personnelles a mis en place des règles et des procédures pour la protection et la gestion des données personnelles sous la supervision du Centre pour la protection des données personnelles. Cette loi a été adoptée dans le cadre de la Convention européenne pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel de 1981 et de son protocole additionnel de 2001, ainsi que de la directive 95/46/CE du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Des instructions pertinentes ont été publiées par le ministère de la Santé à l'intention de toutes les institutions médicales.

MDA / Radu (50073/07)

Arrêt définitif le 15/07/2014

Résolution finale CM/ResDH(2017)347

Les documents médicaux en cause ont été détruits par l'employeur.

L'affaire concernait la divulgation, par un hôpital public à la police, des données médicales des requérants relatives à leur traitement pour toxicomanie. En 2013, un nouveau Code de procédure pénale est entré en vigueur, prévoyant la supervision par les procureurs publics de l'accès de la police aux données personnelles. En 2019, le Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STCE n° 223) a été signé. En 2020, une loi sur la protection des données personnelles a été adoptée, mettant en œuvre les règlements pertinents de l'UE dans le domaine de la protection des données personnelles. L'Agence de protection des données personnelles a adopté des règles sur le traitement des données et sur les évaluations d'impact de la protection des données. En 2021, une loi sur la protection des personnes physiques à l'égard du traitement des données personnelles par les autorités compétentes à des fins de prévention, d'enquête, de détection ou de poursuite d'infractions pénales ou d'exécution de sanctions pénales était en préparation.

MKD / J.M. et A.T. (79783/13)

Arrêt définitif le 22/10/2020

Résolution finale CM/ResDH(2021)123

L'affaire concernait la violation du droit à la vie privée des requérants, ni suspects ni accusés dans une quelconque enquête, en raison de la divulgation de leur dossier médical aux procureurs. La Cour a conclu que la collecte par le bureau du procureur d'informations médicales confidentielles concernant ces requérants n'était pas accompagnée de garanties suffisantes pour empêcher une divulgation incompatible avec le respect de leur vie privée.
Les autorités ont fait référence à un certain nombre d'actes législatifs et réglementaires concernant les soins de santé et la protection des données à caractère personnel qui ont été adoptés ou modifiés à la suite de l'arrêt de la Cour. En particulier, elles ont fait référence à une instruction spéciale de 2013 adressée par le Procureur général aux procureurs sur la collecte et le traitement des données médicales personnelles. Ils ont également cité la jurisprudence des tribunaux internes qui est alignée sur la jurisprudence de la Cour européenne. L'arrêt a été publié et diffusé.

RUS / Avilkina et autres (1585/09)

Arrêt définitif le 07/10/2013

Rapport d'action DH-DD(2014)1329

L'affaire concernait le refus des autorités d'accorder à la requérante l'accès à son rapport médical après examen en prison pour des raisons de sécurité et d'ordre public sur la base d'une circulaire de la Direction générale des grisons et lieux de détention de 1990. À partir de 2005, le Code d'exécution des peines et des mesures de sécurité ainsi que le Règlement sur l'administration des établissements et l'exécution des peines et des mesures de sécurité et la circulaire du ministère de la Justice de 2007 accordent aux détenus le droit d'obtenir l'accès à leur dossier médical et de prendre des copies des documents joints.

TUR / Usla n° 2 (23815/04)

Arrêt définitif le 20/04/2009

Résolution finale CM/ResDH(2014)129

L'affaire concernait la collecte, la conservation et l'utilisation illégales de données sensibles, obsolètes et non pertinentes concernant la santé mentale du requérant (en particulier le certificat du bureau d'enrôlement militaire confirmant l'inaptitude du requérant au service militaire), dans le cadre de l'examen de sa demande de promotion dans une société d'État, ainsi que l'absence de réponse des tribunaux internes aux principaux arguments du requérant présentés dans le cadre de la procédure civile de protection des données contre son employeur.
La Constitution de 1996, modifiée en 2004 et 2014, prévoit que la collecte, la conservation, l'utilisation et la diffusion d'informations confidentielles sur une personne sans son consentement ne sont pas autorisées, sauf si la loi le prévoit dans l'intérêt de la sécurité nationale, du bien-être économique et des droits de l'homme. La loi de 2010 sur la protection des données personnelles prévoit que les informations personnelles ne sont traitées qu'à des fins spécifiques et légitimes avec le consentement de la personne et que le traitement des informations personnelles, en particulier les informations sur l'état de santé, est interdit.

UKR / Surikov (42788/06)

Arrêt définitif le 26/04/2017

Rapport d'action DH-DD(2021)1012

En 2017, le Registre d'État unifié des recrues, des conscrits et des réservistes a été créé en tant que système informatique automatisé pour collecter, stocker, traiter et utiliser les données sur le personnel militaire. La divulgation illégale de données personnelles entraîne une responsabilité administrative et civile. Le Commissaire du Parlement pour les droits de l'homme contrôle également le respect de la législation sur la protection des données.

1.5. Accès et effacement ou destruction de données personnelles

L'affaire concernait l'enregistrement du nom du requérant dans un registre de police des « délinquants » après son interrogatoire par la police sans acte d'accusation officiel et l'absence de recours effectif à cet égard.
Enfin, le nom du requérant a été rayé des registres de police en 2002. L'instruction confidentielle contestée du ministre de l'Intérieur de 1993 comme base légale de l'enregistrement a été révoquée en 2002. La loi sur le ministère de l'Intérieur comme nouveau cadre juridique a été adoptée en 2006. En vertu d'un décret pour l'enregistrement de la police de 2011, les données personnelles ne peuvent être enregistrées que lorsque des chefs d'accusation sont portés en relation avec un crime intentionnel grave. Les autorités de police, d'office ou à la demande de la personne concernée, sont tenues de mettre fin à l'enregistrement de la police lorsque les procédures pénales en jeu sont classées ou que la personne est acquittée. Les refus peuvent faire l'objet d'un recours devant les tribunaux administratifs. La Commission pour la protection des données personnelles, créée en vertu de la loi de 2006 sur la protection des données personnelles interdisant le traitement des données à des fins autres que celles pour lesquelles les informations ont été initialement collectées, surveille les décisions d'enregistrement de la police prises par le ministère de l'Intérieur.

BGR / Dimitrov-Kazakov (11379/03)

Arrêt définitif le 10/05/2011

Résolution finale CM/ResDH(2013)119

L'affaire concernait l'impossibilité de demander l'effacement d'informations enregistrées dans la base de données de la police STIC (système de traitement des infractions constatées) malgré l'abandon des procédures pénales à l'encontre du requérant, depuis 20 ans. Pour exécuter l'arrêt de la Cour européenne, la durée de conservation des données enregistrées n'a pas été légalement modifiée, cependant, les décisions de classement sans suite sont systématiquement mentionnées au dossier depuis 2011. Par ailleurs, la loi de 2016 relative à la lutte contre le crime organisé, le terrorisme et leur financement, permet au procureur d'accorder une requête d'effacement anticipé si l'affaire concernée a fait l'objet d'un non-lieu pour un motif autre que l'insuffisance des chefs d'accusation. La décision du procureur de la République relative à l'effacement ou à la rectification des données personnelles peut faire l'objet d'un recours devant les tribunaux.

FRA / Brunet (21010/10)

Arrêt définitif le 18/12/2014

Résolution finale CM/ResDH(2018)156

L'affaire concernait l'impossibilité légale pour un enfant abandonné à la naissance d'avoir accès aux informations sur ses origines ou de faire une demande de renonciation à la confidentialité des informations par sa mère biologique. Le tribunal a critiqué un manque de proportionnalité entre les intérêts de l'enfant et ceux de la mère biologique, qui souhaitait que son identité reste confidentielle et que l'enfant n'ait pas accès à son testament.
En 2015, suite à l'arrêt de la Cour, le tribunal pour mineurs de Trieste a communiqué à la requérante l'identité de sa mère. En 2013, la Cour constitutionnelle a déclaré inconstitutionnelle la disposition légale, introduite en 2003, qui empêchait un enfant abandonné à la naissance d'avoir accès aux informations sur sa mère biologique sans accorder au juge la possibilité de

ITA / Godelli (33783/09)

Arrêt définitif le 18/03/2013

Résolution finale CM/ResDH(2015)176

vérifier la volonté de la mère biologique. En 2015, un projet de loi sur la procédure de demande d'informations concernant ses origines a été approuvé par la Chambre des Délégués.

L'affaire concernait le refus des autorités, pendant plus de dix ans, d'accorder à la requérante - qui niait toute collaboration avec les services de sécurité à l'époque communiste - l'accès à tous les documents la concernant, collectés par ces services. La Cour a noté, en particulier, l'absence de mise en place d'une procédure efficace permettant aux intéressés d'obtenir l'accès aux documents des services de sécurité les concernant et a confirmé l'approche adoptée dans des affaires précédentes concernant des requérants cherchant à accéder à leurs dossiers créés par les services secrets sous un régime totalitaire.
Suite à l'arrêt de la Cour, la requérante s'est vu accorder l'accès à des copies de tous les documents la concernant qui avaient été créés par les services de sécurité communistes.
En 2010, la loi sur l'Institut du souvenir national de 1998 a été modifiée pour prévoir un droit d'accès aux documents déposés auprès de l'Institut. Ainsi, toute personne a le droit de demander l'accès aux documents qui ont été déposés à l'Institut et qui la concernent. Ces documents sont rendus accessibles par acte administratif avec un droit de recours auprès du président de l'Institut du souvenir national. La décision du président de l'Institut du souvenir national peut faire l'objet d'un recours devant les tribunaux administratifs.

POL / Joanna Szulc (43932/08)

Arrêt définitif le 13/02/2013

Résolution finale CM/ResDH(2014)60

L'affaire concernait une procédure administrative excessivement longue pour traiter une demande d'accès à des informations personnelles recueillies par les services secrets communistes. Afin de permettre un accès effectif aux dossiers, le Conseil national pour l'étude des archives de la *Securitate* a poursuivi le processus d'inventaire des documents transférés des archives de la *Securitate*. Un inventaire des affaires relatives aux questions pénales a été publié sur son site Internet. Un nouveau système technique a été mis en place pour la gestion et la numérisation des documents. La durée moyenne des procédures d'accès a été réduite à une période comprise entre deux et six mois. Tous les dossiers de la *Securitate* ont été transférés au Conseil national, à l'exception de ceux contenant des informations classifiées relatives à la sécurité nationale. Les demandes d'information des parties intéressées doivent être traitées dans un délai de 30 jours.

ROM / Haralambie (21737/03)

Arrêt définitif le 27/01/2010

Résolution finale CM/ResDH(2017)237

L'affaire concernait l'insuffisance des garanties contre l'ingérence arbitraire dans le droit à la vie privée du requérant en raison de la conservation et de la divulgation publique d'informations privées par le service de renseignement roumain, en sa qualité de gardien des archives de l'ancien service secret communiste (la *Securitate*).Suite à l'arrêt, les inscriptions dans les registres ayant entraîné la désignation trompeuse du requérant comme membre d'une organisation d'extrême droite d'avant-guerre ont été modifiées afin d'éviter toute confusion supplémentaire en raison de la similitude des noms. En 2008, le Parlement a réformé le cadre juridique du traitement des informations contenues dans les archives de la *Securitate*. En vertu du règlement de 2008, le traitement de ces informations a été transféré à un organe administratif civil (le Conseil national pour l'étude des archives de la *Securitate* – « NCSAS »), chargé de permettre et de réglementer l'accès aux dossiers de surveillance. Les personnes intéressées peuvent déposer une demande écrite d'accès ou de rectification des informations auprès du NCSAS, qui est contraint de répondre dans les 30 jours et dont les décisions sont soumises à un contrôle judiciaire.

ROM / Rotaru (28341/95)

Arrêt définitif le 04/05/2000

Résolution finale CM/ResDH(2014)253

L'affaire concernait le stockage injustifié par le Service de sécurité d'informations sur les anciennes activités politiques des requérants et le refus d'accorder l'accès à l'ensemble des informations personnelles contenues dans ces dossiers ainsi que l'absence de tout recours effectif.
Suite à l'arrêt de la Cour, les informations sur les requérants ont été supprimées des dossiers du Service de sécurité et ne sont donc ni consultables ni accessibles au personnel du Service de

SWE / Segerstedt-Wiberg et autres (62332/00)

Arrêt définitif le 06/09/2006

sécurité. En janvier 2008, la Commission sur la sécurité et la protection de l'intégrité, nouvellement créée, a commencé sa fonction de contrôle visant également à améliorer l'accès individuel aux recours juridiques internes. Elle supervise le traitement des données personnelles par le Service de sécurité et, après 2012, également par la Police.
Depuis janvier 2007, il est possible d'introduire un recours devant un tribunal administratif général contre une décision du Service de sécurité de ne pas corriger ou supprimer des données à caractère personnel prétendument traitées en violation de la législation.
Enfin, en 2012, la loi sur les données de police est entrée en vigueur. Son objectif général est de protéger la vie privée lorsque des données personnelles sont traitées dans le cadre d'activités répressives. Son contenu coïncide en grande partie avec la législation précédente, mais fournit des réglementations plus claires et plus détaillées dans certains domaines, notamment la suppression des données.

Résolution finale CM/ResDH(2012)222

L'affaire concernait le manquement à l'obligation positive de mettre en place une procédure efficace et accessible permettant au requérant, ancien ingénieur royal de l'armée britannique, d'avoir accès à toutes les informations pertinentes et appropriées lui permettant d'évaluer tout risque auquel il avait été exposé lors de sa participation à des essais de gaz moutarde et de gaz neurotoxique au *Chemical and Biological Defence Establishment* de Porton Down.
Pour éviter des violations similaires, la loi sur la protection des données de 1998 (entrée en vigueur en 2000) a introduit un droit de recevoir ses données personnelles détenues par une autorité publique. Il est possible de faire appel auprès du Commissaire à l'information, une autorité de contrôle indépendante qui rend compte directement au Parlement. Les décisions du Commissaire à l'information peuvent faire l'objet d'un appel devant le Tribunal de l'information. Une commission d'appel distincte du Tribunal, chargée de la sécurité nationale, peut entendre les audiences relatives aux exemptions de divulgation pour des raisons de sécurité nationale.
La loi sur la liberté d'information de 2000 (entrée en vigueur en 2005) a créé un droit général d'accès à toute information détenue par une autorité publique. La procédure d'appel est similaire à celle de la DPA 1998. En vertu de la loi sur les droits de l'homme de 1998 (entrée en vigueur en 2000), un contrôle judiciaire des actions des autorités peut également être demandé auprès du tribunal administratif.
En outre, la ligne d'assistance téléphonique pour les volontaires de Porton Down a été mise en place en février 1998, dans le but d'aider les anciens volontaires ou leurs représentants à accéder facilement aux informations relatives à leur participation aux tests à Porton Down. Enfin, les procédures concernant les demandes d'information sur l'exposition réelle ou possible d'une personne à un danger ont été simplifiées.

UK. / Roche (32555/96)

Arrêt définitif le 19/10/2005

Résolution finale CM/ResDH(2009)20

---

2. SURVEILLANCE SECRÈTE

2.1. Interception de communications et de données personnelles

L'affaire concernait le grief de la requérante selon lequel la police n'avait pas disposé d'une commission rogatoire valide pour la placer sous surveillance secrète dans le cadre d'une enquête pénale sur des allégations de corruption. Les mesures comprenaient l'utilisation d'appareils d'enregistrement lors d'une rencontre avec la requérante, l'interception de conversations téléphoniques et l'enregistrement vidéo de la remise de l'argent du pot-de-vin, remis en billets de banque marqués. Le tribunal a critiqué, en particulier, le fait que le mandat était trop vague, manquant de détails concernant l'objet de la mesure de surveillance, ainsi que l'insuffisance du contrôle judiciaire. Pour prévenir des violations similaires, à partir de 2010, le déroulement pratique des activités opérationnelles et de renseignement a été amélioré en ce qui concerne la procédure, l'autorisation des opérations, la documentation des résultats ainsi que la supervision par la Direction générale de la police criminelle. En mars 2020, le collège des procureurs généraux a assuré le contrôle de la légalité des activités opérationnelles et de renseignement par les procureurs. Le Code de procédure pénale de 2021 comprend des règles générales et des garanties détaillées concernant les mesures opérationnelles et de renseignement (actions d'investigation sous couverture) qui, dans le cadre d'une procédure pénale, ne peuvent être exécutées que sur instruction de l'enquêteur et sur la base d'une décision du tribunal.

ARM / Hambardzumyan (43478/11)

Arrêt définitif le 05/03/2020

Résolution finale CM/ResDH(2021)302

L'affaire concernait des actes illicites accomplis par les autorités dans le cadre d'enquêtes pénales, à savoir l'obtention et l'utilisation de la liste des appels téléphoniques du requérant et l'enregistrement d'une conversation au moyen d'un dispositif d'écoute placé sur le corps, sans base juridique valable pour l'un ou l'autre.
En vertu du Code de procédure pénale de 2002, un juge peut accorder l'accès à des données de télécommunications par une ordonnance écrite motivée. Les conditions d'utilisation des dispositifs de surveillance (appelés « moyens d'investigation opérationnels ») par la police dans le cadre de procédures concernant des infractions pénales intentionnelles y sont également définies. L'autorisation d'un procureur est nécessaire pour la surveillance audio et vidéo des personnes et des objets ; l'autorisation d'un juge est nécessaire pour l'atteinte au domicile ou à la correspondance. Le bureau du procureur suprême a publié des conseils d'interprétation en 2004. L'arrêt a été traduit, publié et diffusé à toutes les autorités concernées.

CZE / Heglas (5935/02)

Arrêt définitif le 09/07/2007

Résolution finale CM/ResDH(2011)98

L'affaire concernait l'absence de motivation suffisante dans les autorisations, par les juges d'instruction et les procureurs, de différentes mesures de surveillance secrète dans le cadre de procédures pénales. La Cour européenne a constaté une ingérence illégale dans le droit à la vie privée malgré l'acceptation - par les tribunaux internes - des justifications rétroactives de ces mesures.
Un amendement au Code de procédure pénale de 2013 prévoit clairement que l'utilisation d'informations obtenues par des activités de surveillance comme pièces à conviction nécessite une autorisation préalable. La Cour suprême a modifié sa jurisprudence en 2017, en soulignant que le contrôle judiciaire à posteriori ne peut pas éliminer l'irrecevabilité des pièces à conviction obtenues sans autorisation préalable et suffisamment motivée. En outre, aux termes de la loi de 2015 sur l'indemnisation des dommages causés dans le cadre de procédures d'infraction, une indemnité peut également être demandée pour les dommages causés par des activités de

EST / Libik et autres (173/15)

Arrêt définitif le 07/10/2019

Résolution finale CM/ResDH(2021)58

surveillance illégales. Des formations et des activités de sensibilisation pertinentes ont été organisées pour les juges, les procureurs et les avocats.

L'affaire concernait la géolocalisation en temps réel du véhicule du requérant en tant que mesure de surveillance prise dans le cadre d'une enquête pénale sur son implication dans des infractions internationales liées au trafic de stupéfiants sur la base d'une loi qui, à l'époque pertinente avant 2014, n'indiquait pas avec suffisamment de clarté dans quelle mesure et comment les autorités étaient autorisées à faire usage de leur pouvoir discrétionnaire. Le jugement a été publié et diffusé à toutes les autorités concernées, y compris le procureur général. En 2014, une loi sur la géolocalisation est entrée en vigueur qui a placé une telle mesure, nécessitant une autorisation suffisamment motivée par un magistrat, sous contrôle judiciaire.

FRA / Ben Faiza (31446/12)

Arrêt définitif le 08/05/2018

Résolution finale CM/ResDH(2021)369

L'affaire concernait l'écoute et l'enregistrement illégaux de la conversation téléphonique du requérant par la police au cours de la procédure pénale engagée contre lui, la loi interne n'indiquant pas avec une clarté raisonnable le champ et les modalités d'exercice de la marge d'appréciation conférée aux autorités publiques.
Afin de prévenir des violations similaires, la loi de 1991 relative au secret des télécommunications a modifié le Code de procédure pénale relatif aux interceptions ordonnées par l'autorité judiciaire. Ainsi, le juge d'instruction peut, si la peine encourue est égale ou supérieure à deux ans d'emprisonnement, ordonner l'interception, l'enregistrement et la transcription des télécommunications. La décision d'interception, qui doit être prise par écrit, n'a pas de caractère judiciaire et n'est pas susceptible de recours. La décision doit contenir tous les éléments permettant l'identification de la ligne téléphonique à intercepter et énoncer l'infraction qui justifie cette mesure. Elle doit également préciser sa durée (une période maximale de quatre mois, renouvelable une fois). Chacune des opérations d'interception et d'enregistrement doit être mentionnée sur un procès-verbal qui précise le jour et l'heure de son début et de sa fin. Les enregistrements seront détruits à l'initiative du ministère public après l'expiration du délai de prescription de l'action publique. Aucune ligne téléphonique vers le cabinet d'un avocat ou son domicile ne peut être interceptée sans que le bâtonnier en ait été préalablement informé par le juge d'instruction.

FRA / Kruslin (11801/85)

Arrêt définitif le 24/04/1990

Résolution finale CM/ResDH(92)41

L'affaire concernait une utilisation illégale de dispositifs d'écoute dans une procédure pénale, dans l'appartement d'un tiers intervenant régulièrement visité par un suspect de meurtre, sur la base d'une réglementation peu claire concernant le pouvoir discrétionnaire des autorités en matière de surveillance audio.
Des mesures relatives à l'utilisation de dispositifs d'écoute dans le cadre de procédures liées à la criminalité organisée ont été introduites dans le Code de procédure pénale en 2004, précisant les catégories de personnes pouvant faire l'objet de telles mesures et la nature des infractions qui pourraient les justifier. Cette loi s'applique également aux parloirs des maisons de correction (lieux publics). Elle prévoit un délai pour les opérations et détermine les conditions d'effacement ou de destruction des enregistrements. La cour de cassation et le Conseil constitutionnel ont modifié leur jurisprudence respective en conséquence.

FRA / Vetter 59842/00

Arrêt définitif le 31/08/2005

Résolution finale CM/ResDH(2010)5

L'affaire concernait la fuite aux médias des conversations téléphoniques du requérant (un homme politique et membre fondateur du parti politique des Libéraux Démocrates), qui avaient été interceptées par le département de la sécurité de l'État et l'absence de recours effectif permettant un examen de la légalité des mesures de surveillance. En 2013, la loi sur le renseignement criminel a prévu des recours internes effectifs, permettant un examen judiciaire de la légalité et de la mise en œuvre des mesures de surveillance. En juin 2015, la Cour suprême a publié sur son site internet une étude de la jurisprudence interne relative au Code de procédure pénale et à la loi sur le renseignement criminel en ce qui concerne la surveillance,

LIT / Draksas (36662/04)

Arrêt définitif le 31/10/2012

Résolution finale CM/ResDH(2016)124

l'enregistrement et le stockage des informations transmises par les réseaux de communications électroniques, et a fourni des informations concernant les critères requis pour que les mesures de surveillance secrète soient conformes à l'article 8.

LVA / Santare et Labaznikovs (34148/07)

Arrêt définitif le 30/06/2016

Résolution finale CM/ResDH(2017)213

L'affaire concernait une ingérence arbitraire, due à l'impossibilité pour les requérants de vérifier si l'interception secrète de conversations téléphoniques dans le cadre de la procédure pénale avait été effectuée sur la base d'une autorisation judiciaire préalable et à l'absence de contrôle effectif par les tribunaux internes de la légalité de la mesure contestée, contrairement aux dispositions légales existantes.
Le Code de procédure pénale de 2005 prévoit que, lorsque des informations obtenues par des mesures de surveillance sont utilisées comme pièces à conviction dans le cadre d'une procédure pénale, le dossier de l'affaire doit inclure une lettre de référence avec l'autorisation mentionnant l'institution autorisant la mesure, ainsi que la date et la période pour lesquelles la mesure a été autorisée. Ces lettres de référence, délivrées par la Cour suprême, permettent aux personnes concernées de vérifier si la pièce à conviction a été obtenue dans le respect de la procédure prescrite. Les amendements de 2014 au Code de procédure pénale ont élargi la compétence du pouvoir judiciaire en ce qui concerne la recevabilité des preuves obtenues à la suite de mesures opérationnelles spéciales : sur une demande défendable du procureur, de la victime, du prévenu ou de l'avocat de la défense, le tribunal de première instance doit prendre en considération les documents résultant d'une enquête spéciale classée liée aux pièces à conviction utilisées dans la procédure pénale.

LVA / Meimanis (70597/11)

Arrêt définitif le 21/10/2015

Résolution finale CM/ResDH(2017)211

L'affaire concernait l'interception illégale des conversations téléphoniques sur le téléphone portable du requérant sans approbation judiciaire *ex post facto*, dans le cadre d'une enquête opérationnelle menée par le Bureau de prévention et de lutte contre la corruption pour tentative d'acceptation d'un pot-de-vin. La violation avait résulté d'une incohérence entre les termes de la loi sur les activités opérationnelles en vigueur au moment des faits et la pratique des autorités répressives internes, selon laquelle une approbation *ex post facto* des autorités judiciaires n'était pas demandée dans toutes les affaires, en particulier lorsque les activités opérationnelles étaient terminées dans les 72 heures et qu'aucune prolongation n'était nécessaire.
En juin 2011, la Cour constitutionnelle a jugé qu'une approbation judiciaire *ex post facto* des mesures opérationnelles doit toujours être obtenue par le président de la Cour suprême (ou un juge spécialement autorisé), même si la mesure en question a été classée en moins de 72 heures. Les autorités internes sont liés par cette interprétation. L'arrêt a été publié et largement diffusé à tous les tribunaux et autorités judiciaires concernés.

NLD / R.V. et autres (14084/88)

Décision définitive le 15/05/1992

Résolution finale CM/ResDH(2007)88

La violation constatée dans cette affaire concernait la surveillance - en vertu d'un décret de 1972 sur les services de renseignement et de sécurité - des activités des requérants par les services de renseignement et de sécurité ainsi que le refus d'accès à la compilation et la conservation d'informations personnelles les concernant.
La loi de 1988 sur les services de renseignement et de sécurité contenait des modifications substantielles concernant les conditions dans lesquelles les informations obtenues peuvent être enregistrées et transmises à d'autres organismes ou personnes. Toutefois, la loi n'a introduit aucun changement en ce qui concerne les circonstances dans lesquelles des modes de surveillance secrets peuvent être déployés.
En 2002, la loi sur les services de renseignement et de sécurité a défini les circonstances et les conditions habilitant les autorités à effectuer des mesures de surveillance secrète et a établi la procédure concernant les demandes d'accès aux dossiers des services de sécurité, y compris l'appel. La loi a également fourni une définition des personnes susceptibles d'être soumises à des mesures de surveillance secrète et une description des moyens à employer à cette fin. Selon la loi, les services de sécurité doivent publier un rapport annuel qui est soumis au Parlement, dans

lequel les domaines d'attention spécifique concernant les services pour l'année passée et à venir sont soulignés.

L'affaire concernait une ingérence arbitraire dans la vie privée du requérant en raison de la surveillance secrète d'un demandeur d'assurance sociale par des enquêteurs privés, sans clarté juridique suffisante quant au champ et aux modalités d'exercice du pouvoir discrétionnaire conféré aux compagnies d'assurance agissant en tant qu'autorités publiques dans les litiges d'assurance.
En octobre 2016, la Caisse nationale d'assurance accident a annoncé qu'elle cesserait de faire appel à des détectives privés dans la lutte contre la fraude à l'assurance. En 2017, le Tribunal fédéral a rendu deux arrêts de principe selon lesquels la pertinence du présent arrêt s'applique à tous les domaines du droit. En septembre 2019, une modification de la loi fédérale sur les assurances sociales est entrée en vigueur, établissant les bases légales pour la surveillance des assurés. Elle permet en particulier l'enregistrement d'images et de vidéos à des fins d'enquête. Il contient également une liste des mesures possibles soumises à une autorisation judiciaire ou ne nécessitant que la décision d'un gestionnaire d'assurance. En outre, l'amendement énumère les circonstances qui justifient la surveillance, prévoit l'obligation d'informer la personne concernée et établit des règles générales pour le stockage et la destruction des données collectées.

SUI / Vukota-Bojic (61838/10)

Arrêt définitif le 18/01/2017

Résolution finale CM/ResDH(2019)233

L'affaire concernait le manque de prévisibilité de la législation interne concernant la surveillance des lignes téléphoniques d'un avocat, dans le cadre d'une procédure pénale à laquelle il était un « tiers intervenant », et non un suspect, sur ordre du Procureur fédéral.
Le tribunal a estimé que la violation était due à une divergence entre le texte clair de la législation protégeant le secret professionnel des avocats et la pratique suivie, la loi n'indiquant pas clairement dans quelles conditions et par qui la distinction entre les questions liées au travail d'un avocat et celles relatives à ses autres activités doit être établie. En 2002, la loi fédérale sur la surveillance de la correspondance postale et des télécommunications a défini en détail les conditions dans lesquelles les appels téléphoniques peuvent être interceptés. Elle prévoit des exceptions pour lesquelles une autorisation peut être donnée pour surveiller des personnes contraintes au secret professionnel, lorsqu'elles ne sont pas elles-mêmes suspectes ou chefs d'accusation. Si la surveillance d'un avocat révèle des informations relevant du secret professionnel, les documents pertinents doivent être retirés du dossier et ne peuvent être utilisés dans une procédure pénale.

SUI / Kopp (23224/94)

Arrêt définitif le 25/03/1998

Résolution finale CM/ResDH(2005)96

L'affaire concernait le défaut d'obtention par la police d'une ordonnance du tribunal pour accéder aux informations relatives à l'abonné associées à une adresse IP dynamique, enregistrées par les forces de l'ordre suisses lors de leur surveillance des utilisateurs d'un certain réseau de partage de fichiers. Cela a conduit à l'identification du requérant après qu'il a eu partagé des fichiers sur le réseau, y compris de la pornographie enfantine. Le tribunal a constaté en particulier que la disposition légale utilisée par la police pour obtenir les informations sur l'abonné manquait de clarté, n'offrait pratiquement aucune protection contre l'arbitraire, ne comportait aucune garantie contre les abus et ne prévoyait aucun contrôle indépendant des pouvoirs de police impliqués.
La violation en cause résulte en partie des dispositions législatives déficientes et en partie de la jurisprudence inadéquate des tribunaux internes. En vertu des amendements de 2019 du Code de procédure pénale, l'accès aux données relatives au trafic des communications et leur transfert nécessitent une ordonnance du tribunal et sont supervisés par les tribunaux. Toutes les données recueillies par la police doivent être soumises au procureur de la République. La supervision interne au sein de la police et la supervision administrative par le ministère de l'Intérieur doivent également être réglementées. En outre, une lettre circulaire du bureau du procureur général a été adressée aux procureurs et à la police sur les conclusions du tribunal. En juillet 2018, une

SVN / Benedik (62357/14)

Arrêt définitif le 24/07/2018

Résolution finale CM/ResDH(2021)294

instruction contraignante a été émise à l'intention de la police pour qu'elle obtienne une ordonnance préalable du tribunal lorsqu'elle demande des données d'abonnés liées à une adresse IP spécifique. En octobre 2018, la jurisprudence interne a changé, soulignant qu'une ordonnance du tribunal était nécessaire pour obtenir les données d'abonné associées à l'adresse IP dynamique faisant référence à l'arrêt de la Cour.

L'affaire concernait l'existence admise, en Angleterre et au Pays de Galles, de lois et de pratiques permettant l'interception de communications postales et téléphoniques et l'utilisation d'un instrument de « comptage » de téléphones par ou pour le compte de la police dans le cadre d'enquêtes criminelles. La loi de 1985 sur l'interception des communications a mis le droit interne en conformité avec la CEDH. Elle l'a fait en établissant un cadre législatif complet régissant l'interception des communications sur les systèmes publics de poste et de télécommunications, dans lequel les motifs d'interception autorisée sont expressément énoncés, et dans lequel toute interception effectuée autrement que conformément aux dispositions de la loi constitue une infraction pénale.	***UK. / Malone (8691/79)*** ***Arrêt définitif du 26/04/1985*** ***Résolution finale CM/ResDH(86)1***
L'affaire concernait l'ingérence illégale dans le droit à la vie privée des requérants, deux organisations non gouvernementales travaillant dans le domaine des droits de l'homme et établies en Irlande et au Royaume-Uni, en raison de la clarté insuffisante de l'*Interception of Communications Act 1985* qui conférait aux autorités un très large pouvoir discrétionnaire pour surveiller certaines formes de leurs communications électroniques. La loi de 1985 sur l'interception des communications a été remplacée par la loi de 2000 sur la réglementation des pouvoirs d'investigation, qui prévoit des procédures claires pour l'autorisation et le traitement des commissions rogatoires d'interception ainsi que pour le traitement, la communication et la destruction du matériel intercepté.	***UK. / Liberty et autres (58243/00)*** ***Arrêt définitif le 01/10/2008*** **Résolution finale CM/ResDH(2011)83**
L'affaire concernait la surveillance secrète des consultations d'un détenu avec son avocat et la personne désignée pour l'assister, en tant que personne vulnérable, après son arrestation. Le régime juridique ne prévoyait pas de garanties suffisantes pour la protection du matériel obtenu par la surveillance secrète des consultations entre avocats et clients. En 2010, le Code d'application pour le traitement, le stockage et la destruction en toute sécurité du matériel obtenu par la surveillance secrète a été mis en application pour corriger cette lacune juridique. L'arrêt a été publié et diffusé à toutes les autorités concernées.	***UK. / R.E. (62498/11)*** ***Arrêt définitif le 27/01/2016*** **Résolution finale CM/ResDH(2016)143**

2.2. Surveillance sur le lieu de travail

L'affaire concernait la décision d'une société privée de licencier un employé après avoir surveillé ses communications électroniques et accédé à leur contenu, et le manquement des tribunaux internes à protéger son droit au respect de sa vie privée et de sa correspondance. En particulier, les tribunaux nationaux n'avaient pas déterminé si le requérant avait été préalablement informé par son employeur du fait de la surveillance ou s'il avait été informé de la nature ou de l'étendue de la surveillance et du degré d'intrusion. La violation était due à une application erronée du droit interne dans l'affaire en question. L'arrêt a été publié, traduit et diffusé à tous les tribunaux internes. Il est utilisé dans les activités de formation de l'Institut national des juges et des magistrats.	***ROM / Barbulescu (61496/08)*** ***Arrêt définitif le 05/09/2017*** **Résolution finale CM/ResDH(2019)124**

L'affaire concernait l'ingérence arbitraire dans le droit à la vie privée et à la correspondance de la requérante en raison de la surveillance de son téléphone, de son courrier électronique et de son utilisation d'Internet pendant la durée de son emploi par un organisme public, à son insu et sans qu'aucune loi interne ne soit en place pour réglementer une telle surveillance.
La loi de 2000 sur les pouvoirs d'investigation (*Regulation of Investigatory Powers Act*) prévoit la réglementation de l'interception des communications. Le Règlement sur les télécommunications de 2000 définit les circonstances dans lesquelles les employeurs peuvent enregistrer ou surveiller les communications des employés (comme les e-mails ou le téléphone) sans le consentement de l'employé ou de l'autre partie à la communication. Des directives sur la surveillance de l'utilisation de la technologie par le personnel ont été mises en place et comprennent l'obligation d'informer le personnel des interceptions effectuées en vertu du Règlement sans consentement. Pour les interceptions hors du champ d'application du Règlement, le consentement de l'expéditeur et du destinataire est requis et peut être obtenu par l'insertion d'une clause dans les contrats du personnel et par les opérateurs d'appels indiquant que les appels peuvent être surveillés ou enregistrés, à moins que des tiers intervenants ne s'y opposent.

UK. / Copland (62617/00)

Arrêt définitif le 03/07/2007

Résolution finale CM/ResDH(2010)79

L'affaire concernait une ingérence illégale dans le droit à la vie privée des requérants en raison de l'utilisation par la police de dispositifs d'écoute discrète sur leur lieu de travail ou de résidence, au motif que la base juridique n'était ni contraignante ni accessible au public et que les requérants ne disposaient pas d'un recours effectif puisque la procédure de plainte ne protégeait pas contre les abus d'autorité. Pour prévenir des violations similaires, la partie pertinente de la loi sur la police a été introduite en 1999 ainsi que le Code de pratique sur le travail de surveillance intrusive, tous deux juridiquement contraignants et accessibles. En outre, la loi de 2000 sur la réglementation des pouvoirs d'investigation (*Regulation of Investigatory Powers Act*) a assuré une surveillance indépendante par un commissaire en chef de la surveillance et a établi un tribunal indépendant pour examiner les griefs.

UK.. / Groupe Govell (27237/95)

Arrêt définitif le 18/05/1998

Résolution finale CM/ResDH(2005)68

L'affaire concernait une violation du droit de la requérante au respect de sa vie privée en raison de l'interception, entre 1990 et 1992, des appels téléphoniques qu'elle avait effectués à partir des téléphones de son bureau, qui étaient reliés à des systèmes de télécommunications internes exploités par les autorités publiques. Le tribunal a estimé que cette ingérence était illégale car, à l'époque, la loi interne ne réglementait pas l'interception des appels téléphoniques effectués sur ce type de système de télécommunications. En outre, en raison de l'absence de toute réglementation en la matière, la requérante ne disposait d'aucun recours effectif pour se plaindre de l'interception de ses appels téléphoniques.
Suite à l'arrêt, le matériel intercepté a été détruit.
Une nouvelle législation a été adoptée, la loi de 2000 sur la réglementation des pouvoirs d'investigation (*Regulation of Investigatory Powers Act*), qui prévoyait la réglementation de l'interception des communications. Son objectif était d'interdire l'interception des communications sur les réseaux publics et privés, et d'exclure de cette interdiction générale certaines circonstances limitées dans lesquelles l'interception peut être conforme à la loi sur ces réseaux. L'interception intentionnelle et non autorisée d'une communication au moyen d'un système de télécommunications privé constitue une infraction pénale. La loi a également créé une nouvelle responsabilité civile : l'expéditeur, le destinataire ou le destinataire prévu d'une communication interceptée peut assigner en justice la personne qui a le droit de contrôler le fonctionnement ou l'utilisation du système de télécommunication en question. Cette dernière sera responsable, sauf si elle peut démontrer qu'elle a agi avec une autorité conforme à la loi. L'interception sur un réseau privé effectuée conformément à une commission rogatoire du Secrétaire d'État est conforme à la loi. Depuis l'entrée en vigueur de la loi sur les droits de l'homme en 2000, toute personne peut assigner en justice l'autorité concernée l'*Investigatory Powers Tribunal* est compétent pour les procédures contre les services de renseignement concernant, entre autres, une interception de communications.

UK. / Halford (20605/92)

Arrêt définitif le 25/06/1997

Résolution finale CM/ResDH(2007)15

2.3. Surveillance de masse

BGR / Association pour l'intégration européenne et les droits de l'homme et groupe Ekimdzhiev (62540/00)

Arrêt définitif le 30/01/2008

Plan d'action DH-DD(2019)401

L'affaire concerne la surveillance secrète et le système de conservation et d'accès ultérieur aux données de communication. Les principales lacunes du cadre juridique régissant la surveillance secrète ciblée constatées par le tribunal concernaient : l'absence de contrôle indépendant sur la mise en œuvre des mesures de surveillance secrète ; l'utilisation discrétionnaire de renseignements ne relevant pas du champ d'application de la demande initiale de surveillance ; l'absence de garanties suffisantes en ce qui concerne la surveillance effectuée pour des motifs de sécurité nationale ; l'absence de réglementation précise sur le filtrage, la préservation de la confidentialité et de l'intégrité et la destruction des renseignements recueillis ; l'absence de notification des personnes soumises à la surveillance secrète en dehors des procédures pénales et l'absence de recours effectif.

Jusqu'à présent, les mesures adoptées montrent des progrès considérables, comme l'amélioration des procédures d'autorisation judiciaire (également dans le cadre de la protection de la sécurité nationale), la création du « Bureau national » en tant qu'organe de contrôle, l'introduction d'un recours compensatoire et la diminution du recours à la surveillance secrète.

Suite aux amendements législatifs de 2013 et 2015, les demandes de surveillance doivent être soigneusement motivées et justifiées et ne peuvent être soumises que dans le but de prévenir ou d'enquêter sur une liste exhaustive d'infractions pénales graves. Comme l'a noté le Bureau national de surveillance du système de surveillance secrète, les garanties relatives à l'autorisation judiciaire de surveillance pour la protection de la sécurité nationale sont similaires à celles concernant les affaires pénales. Les délais normaux vont de 20 jours à six mois. En vertu du Code de procédure pénale, les renseignements qui ne relèvent pas du champ d'application de la requête initiale ne peuvent être utilisés que dans la mesure où ils concernent d'autres infractions pénales graves pour lesquelles la surveillance secrète est autorisée. Un délai spécifique de 15 ans pour la conservation des renseignements liés à certaines infractions concernant la sécurité nationale a été introduit en 2015. Le Bureau national notifie d'office les citoyens qui ont fait l'objet d'une surveillance secrète illégale, à défaut de certains intérêts compensatoires. Depuis 2009, il est possible de demander une indemnité pour surveillance secrète illégale. La Cour suprême de cassation a récemment précisé dans sa jurisprudence la définition de l'« illégalité » dans ce contexte.

HUN / Szabo et Vissy (37138/14)

Arrêt définitif le 12/06/2016

Plan d'action DH-DD(2021)89

L'affaire concerne la législation sur les mesures de surveillance secrète à des fins de sécurité nationale introduite en 2011, qui ne prévoyait pas de garanties suffisamment précises, efficaces et complètes sur l'ordonnancement, l'exécution et la réparation éventuelle de ces mesures. Le tribunal a souligné que le champ d'application de ces mesures pouvait inclure pratiquement n'importe qui, les nouvelles technologies permettant au gouvernement d'intercepter facilement des masses de données concernant même des personnes situées en dehors du champ d'opération initial. En outre, l'ordonnance de telles mesures relevait entièrement du domaine de l'exécutif, sans évaluation du caractère strictement nécessaire de l'interception des communications et sans qu'aucune mesure de réparation effective, et encore moins judiciaire, ne soit mise en place.

Les autorités ont reconnu la nécessité de modifier la législation actuelle sur les mesures de surveillance secrète et ont informé le CM des travaux préparatoires en cours à cette fin. En juillet 2018, la disposition contestée sur la collecte de renseignements pour la sécurité nationale dans la loi sur la police a été déplacée dans un chapitre différent de la même loi, le contenu restant inchangé.

L'affaire concernait le refus arbitraire d'accès à des informations obtenues par surveillance électronique par l'Agence de renseignement malgré une ordonnance définitive et contraignante du Commissaire à l'information, un organe interne créé pour assurer le respect de la loi sur la liberté d'information de 2004. La Cour a indiqué, en vertu de l'article 46, que la manière la plus naturelle d'exécuter son arrêt dans cette affaire serait de faire en sorte que l'agence fournisse à l'ONG requérante les informations qu'elle avait demandé sur le nombre de personnes ayant fait l'objet d'une surveillance électronique en 2005.
En exécution de cet arrêt, l'Agence de renseignement a fourni à l'ONG requérante les informations demandées dans une lettre datée du 19 juin 2014. En outre, l'agent du gouvernement a envoyé des directives claires au directeur de l'Agence de renseignement quant à son obligation de se conformer strictement au droit interne et aux normes de la CEDH en ce qui concerne l'accès aux informations recueillies par surveillance électronique.

SER / Youth Initiative for Human Rights (48135/06)

Arrêt définitif le 25/09/2013

Résolution finale CM/ResDH(2018)71

L'affaire concernait le risque allégué que les communications de la fondation requérante soient interceptées et examinées par le biais de signaux de renseignement, étant donné qu'elle communiquait quotidiennement avec des particuliers, des organisations et des entreprises en Suède et à l'étranger par courriel, téléphone et télécopie, souvent sur des sujets sensibles.
Le tribunal a constaté, en particulier, que le régime d'interception massive souffrait de trois déficiences : l'absence d'une règle claire sur la destruction du matériel intercepté ne contenant pas de données personnelles ; l'absence d'une exigence dans la loi sur le renseignement des transmissions ou dans d'autres lois pertinentes selon laquelle, lors de la décision de transmettre du matériel de renseignement à des partenaires étrangers, il faut tenir compte des intérêts de la vie privée des individus ; et l'absence d'un contrôle effectif *a posteriori*. Par conséquent, le système ne répondait pas à l'exigence de garanties « de bout en bout », il dépassait la marge d'appréciation laissée à l'État défendeur à cet égard et, dans l'ensemble, il ne protégeait pas contre le risque d'arbitraire et d'abus.
En janvier 2022, la loi sur le traitement des données personnelles à l'Établissement radio de la défense nationale est entrée en vigueur. Elle contient des dispositions détaillées imposant à l'Établissement radiophonique de la défense nationale, avant de décider de transmettre du matériel de renseignement à des partenaires étrangers, d'analyser et d'évaluer si le destinataire étranger des données assure une protection suffisante de ces données, ce qui permet de remédier en partie aux lacunes identifiées par le tribunal concernant la législation de la transmission de matériel de renseignement à des partenaires étrangers. Une réponse concrète doit encore être apportée en ce qui concerne les autres lacunes constatées par la Cour européenne dans cette affaire.

SWE / Centrum for Rättvisa (35252/08)

Arrêt définitif le 25/05/2021

Plan d'action DH-DD(2021)1287

Cette affaire concerne la divulgation par le premier requérant - un fonctionnaire militaire du Service de renseignement roumain (« SRI ») - d'informations sur des écoutes téléphoniques illégales à grande échelle de la part du SRI et du contenu de certaines des communications ainsi interceptées, y compris des conversations téléphoniques entre les deux autres requérants. Ces révélations lors d'une conférence de presse en 1996 ont abouti à la condamnation du premier requérant, en dernière instance par le Tribunal suprême de justice en mai 2002, à une peine de prison avec sursis. En matière d'interception des communications, la Cour européenne a conclu à la violation des articles 8 et 13 de la Convention en raison de l'absence de garanties dans la législation sur les mesures de surveillance secrète fondées sur des considérations de sécurité nationale, en particulier, en ce qui concerne la collecte et le stockage de données à caractère personnel par le SRI, et de l'absence de recours internes permettant de contester la conservation de ces données par ce dernier.
La loi n° 255/2013, en vigueur depuis le 1er février 2014, a modifié le cadre juridique pertinent, à savoir la loi sur la sécurité nationale et la loi régissant l'organisation et le fonctionnement du SRI, et a remédié à certaines des déficiences relevées par la Cour dans cette affaire et dans d'autres affaires antérieures soulevant les mêmes questions. Cette réforme législative a

ROM / Bucur et Toma (40238/02)

Arrêt définitif le 08/04/2013

Plan d'action DH-DD(2014)636

Communication des autorités sur les mesures générales (modifications législatives) DH-DD(2014)592

notamment introduit l'exigence d'une autorisation judiciaire pour les mesures de surveillance secrète pour des motifs de sécurité nationale, sauf dans les situations d'urgence, où cette autorisation peut être accordée par le procureur pour une durée de 48 heures ; dans cette dernière affaire, l'autorisation du procureur est soumise à un contrôle judiciaire d'office et le juge peut ordonner aux services de renseignement de cesser leurs activités et de détruire les données collectées lorsque l'autorisation a été indûment accordée. L'arrêt a été largement diffusé auprès des tribunaux et des autres autorités compétentes et a été publié au Journal officiel.

UK. / Big Brother Watch et autres (58170/13)

Arrêt définitif le 25/05/2021

Plan d'action DH-DD(2021)1326

L'affaire concerne certaines lacunes du régime de surveillance secrète, notamment l'interception massive et l'obtention de données de communication auprès de fournisseurs de services de communication au Royaume-Uni avant 2018 (violations des articles 8 et 10). Tout en concluant que la Convention n'interdit pas en soi le recours à l'interception de masse pour protéger les intérêts de sécurité nationale et d'autres intérêts nationaux essentiels contre des menaces extérieures graves, le tribunal a souligné la nécessité de « garanties de bout en bout » et a défini l'approche à suivre dans de telles affaires. Le tribunal a estimé que, malgré ses garanties, dont certaines solides, le cadre juridique précédent au Royaume-Uni (*Regulation of Investigatory Powers Act (RIPA) 2000*), qui était en vigueur jusqu'en 2018, ne contenait pas suffisamment de « garanties de bout en bout » pour offrir des garanties adéquates et efficaces contre l'arbitraire et le risque d'abus.
L'*Investigatory Powers Act (IPA)* a remplacé le cadre juridique précédent, la RIPA. Elle a introduit un « double verrou » qui exige que les mandats pour l'utilisation des pouvoirs d'investigation soient autorisés par un Secrétaire d'État et approuvés par un juge du Bureau du Commissaire aux pouvoirs d'investigation. En outre, le Commissaire aux pouvoirs d'investigation assure une surveillance indépendante solide de la manière dont ces pouvoirs sont utilisés. D'autres mesures seront préparées afin de remédier à toutes les lacunes identifiées par le tribunal européen.

Index des affaires

ARM / Hambardzumyan 18
BGR / Association pour l'intégration européenne et les droits de l'homme et groupe Ekimdzhiev 23
BGR / Dimitrov-Kazakov 16
BGR / Groupe Petrov 10
BGR / Krasimir Yordanov 4
BGR / Mironov 10
CYP / Onoufriou 11
CZE / Delta Pekárny a.s. 8
CZE / Heglas 18
ESP / Trabajo Rueda 8
ESP / Vincent Del Campo 4
EST / Libik et autres 18
EST / Slavgorodski 11
EST / Soro 4
FIN / Z. 14
FRA / Aycaguer 4
FRA / Ben Faiza 19
FRA / Brunet 16
FRA / Kruslin 19
FRA / M.K. 5
FRA / Ravon et autres 8
FRA / Slimane-Kaid 11
FRA / Vetter 19
GER / Buck 8
GRC / Groupe Modestou 8
GRC / Peers 11
HUN / Szabo et Vissy 24
HUN / Turan 8
ITA / Calogero Diana 11
ITA / Godelli 16
ITA / Labita 11
LIT / Draksas 19
LIT / Valasinas 12
LVA / Boze 9
LVA / L.H. 14
LVA / Lavents 12
LVA / Meimanis 20
LVA / Santare et Labaznikovs 20
MDA / Bostan 9
MDA / P.T. 14
MDA / Radu 14
MDA / Savotchko 5
MKD / J.M. et A.T 14
NLD / A.B. 12
NLD / R.V. et autres 20
POL / Groupe Klamecki n° 2 12
POL / Joanna Szulc 16
ROM / Barbulescu 22
ROM / Bucur et Toma 25
ROM / Dragos Ioan Rusu 9
ROM / Haralambie 17
ROM / Rotaru 17
RUS / Avilkina et autres 15
RUS / Boris Popov 12
SER / Dragan Petrovic 9
SER / Youth Initiative for Human Rights 24
SUI / Kopp 21
SUI / Vukota-Bojic 21
SVN / Benedik 21
SWE / Centrum for Rättvisa 24
SWE / Segerstedt-Wiberg et autres 17
TUR / Alkaya 5
TUR / Groupe Tamer 13
TUR / Sinan Isik 5
TUR / Tarman 5
TUR / Usla n° 2 15
UK. / Big Brother Watch et autres 25
UK. / Catt 6
UK. / Copland 22
UK. / Gaughran 6
UK. / Halford 23
UK. / Liberty et autres 22
UK. / M.M. 6
UK. / Malone 21
UK. / Peck 7
UK. / R.E. 22
UK. / Roche 17
UK. / S. et Marper 7
UK. / Szuluk 13
UK. /Groupe Govell 23
UKR / Golovan 10
UKR / Les affaires du groupe Koval et autres 10
UKR / Mikhaylyuk et Petrov 13
UKR / Panteleyenko 9
UKR / Surikov 15
UKR / Volokhy 10
UKR / Voskoboynikov 10