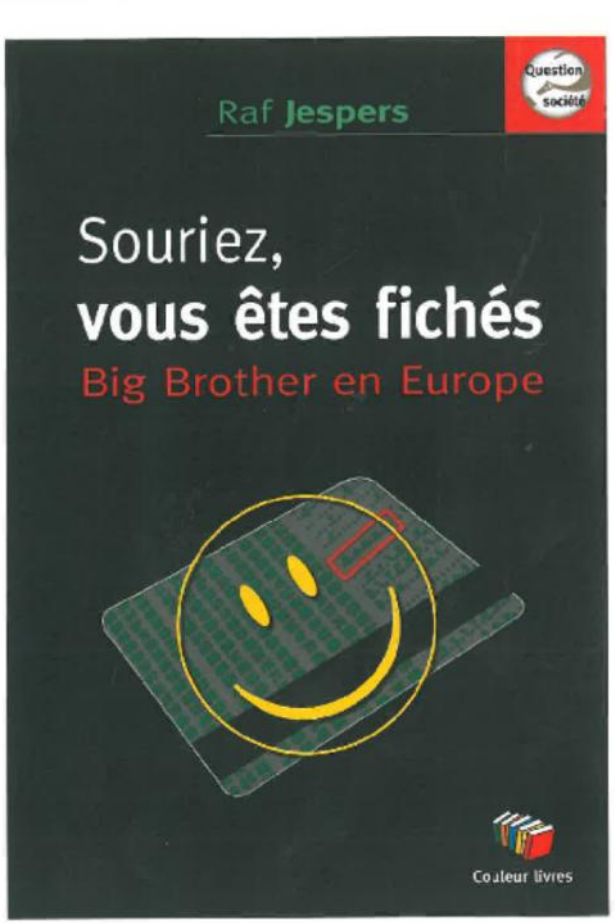
Justifications sécuritaires aux atteintes à la vie privée: construction et déconstruction

- Raf Jespers
- Avocat PROGRESS Lawyers Network
- Auteur: *'Souriez, vous êtes fichés. Big Brother en Europe'* (Couleur livres, 2013)


Raf Jespers
Question de société
Souriez,
vous êtes fichés
Big Brother en Europe
Couleur livres

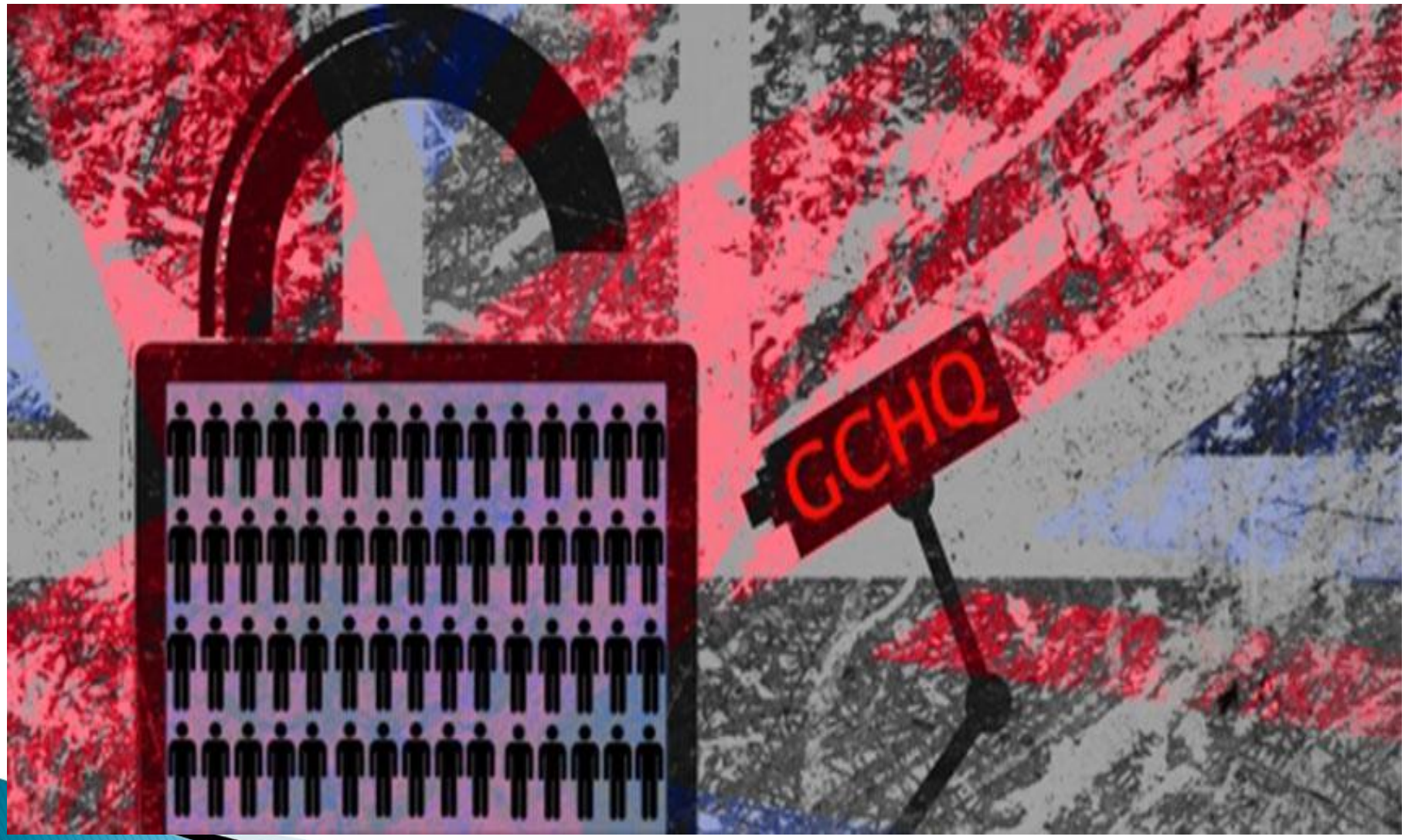
- 1. Stratégie de la tension et de la peur
- 2. Mesures antiterroristes: politique globale de contrôle de la population
- 3. La résistance juridique
- 4. La résistance des citoyens

1. Stratégie de la tension et de la peur: 'war' on terror

- Stratégie connue: Bande de Nivelles (1982-1985), CCC (1984-1985), gare de Bologne (1980), Brigades Rouges (1970-1980)
- 9/11, Madrid (2003), Londres (2005), Charlie Hebdo (2015), musée juif (2014), Thalys (2015)
- Réfugiés
- Menaces de la sécurité: terrorisme, masse de réfugiés
- Base: peur crise, futur, climat, insécurité sociale…

2. Mesures antiterroristes: politique globale de contrôle de la population

- Après 9/11: mondialise combat contre le terrorisme; histoire sans fin; (avant: localisés, temporaires)
- Révélations NSA/GCHQ; Merkel, Belgacom…
- UE: mesures antiterroristes; l'ensemble de la population sous contrôle; double agenda, large spectre


GCHQ

Terror Attacks Around the World

Year	Number of Terror Attacks	Number Killed
2001	355	3295
2002	199	725
2003	208	625
2004	650	1907
2005	11000	14200
2006	14000	20000
2007	14415	22720
2008	11663	15709
2009	10968	15311
2010	11641	13193
2011	10283	12533
2012	6771	11000
2013	10000	18000
2014	13500	32727

Causes augmentation terror attacks ?

- 'Iraq Effect': augmentation après l'invasion de 2003
- War on terror: entre 1,3 et 2 millions de morts en Iraq, Afghanistan et Pakistan
- Guerre permanent en Afghanistan, Iraq, Syrie.
- Déstabilisation Libye
- Nouvelle génération de chefs et d'opérations terroristes

Réponse des autorités apres 9/11

- UE: plus que 200 mesures: nouvelles lois pénal antitéroristes (144 lois 2012); dataretention directive; PNR accords; collaboration internationale; développement Europol, Eurojust, Frontex…

- Belgique: loi antitéroriste (2 élargissements); loi dataretention;

Edward Snowden speech 17.12.2013

These programs were never about terrorism: they're about economic spying, social control, and diplomatic manipulation. They're about power.

Réponse des autorités après Charlie Hebdo: UE

- Le retour du même sans evaluations des > 200 mesures prises.
- Paul De Hert: 'Cessez d'adopter sans cesse de nouvelles mesures, et veillez à ce que celles qui existent déjà fonctionnent réellement'.
- UE: (note Conseil européen 17.1.2015): 'intervenir plus rapidement et plus efficacement';
- – prévention de la radicalisation (internet; médias sociaux); deradicalisation; contrôle total de l'internet; avec Etats-Unis;
- – neutraliser les facteurs sous-jacents: éducation, formation, travail, intégration
- – contrôle renforcé aux frontières
- – collecte intensifiée d'informations; E-PNR

Réponse des autorités après Charlie Hebdo: Belgique (1)

- 'Sécurité Intégrale': collaboration avec les autorités locales et entités fédérées; Conseil National de Sécurité; Plan national 2017

- <u>12 mesures</u>

- 1. optimaliser l'échange d'informations entre les services et institutions administratifs et judiciaires;

- 2. Conseil National de Sécurité (NSA?) Branche politique; branche administrative; centralisation inédite des renseignements et pouvoirs; déterminer le niveau de la menace

Réponse des autorités après Charlie Hebdo: Belgique (2)

- **3.** Elargir écoute téléphonique; extension des méthodes particulières de recherches aux nouveaux délits térroristes (2013: incitation, recrutement; entraînement)

- **4.** Nouveau délit terroriste: déplacement à l'étranger dans des buts terroristes

- **5.** Déchéance de la nationalité belge; double peine; contre le droit international et le droit de l'UE

Réponse des autorités après Charlie Hebdo: Belgique (3)

- 6. Retirer provisoirement des cartes d'identité; ne pas délivrer de passeports.
- 7. Geler les avoirs nationaux ou les fonds qui auraient un lien avec le terrorisme.
- 8. Plus de kaki en rue; pour des manoeuvres statiques; paracommandos/armée; De Wever: blocages des forains; exercises port d'Anvers; impact énorme sur l'atmosphère sociale; légale? Niveau de menace 3; guerre, ennemi intérieur


Politie

Réponse des autorités après Charlie Hebdo: Belgique (4)

- 9. attaquer radicalisation salafiste en prison; unités séparées
- 10. lutte contre radicalismes, au pluriel; l'oeuf de Colomb; pas de définition; politique préventive et proactive tant sur le plan judiciaire que sur le plan administratif
- 11. Révision plan R de 2005 contre radicalisation
- 12. Révision circulaire 'Foreign Fithers' du 25 septembre 2014

Conclusions? Que faire ?

- La lutte contre le terrorisme est un but légitime; les autorités doivent garantir la sécurité des citoyens; pas être naïf
- Politique sécuritaire doit respecter les droits démocratiques et fondamentaux, e.a. le droit à la vie privée; respecter les acquis progressives du droit internationale e.a. des années après guerre
- Attention aux effets contre-productifs et aux dommages collatéraux

Conlusions? Que faire?

- Dénoncer le double agenda politique, des agenda's cachés (controle social, répression lutte sociale et opposition politique…)
- Défendre approche sécuritaire basée sur la prévention, par la collecte, l'échange et la cartographie d'informations
- Abrogation des législations et mesures d'exception
- S'attaquer aux causes du terrorisme et de l'immigration
- Coolsaet: le terrorisme à travers l'histoire; terrorisme anarchiste a connu un revers énorme à partir du moment où le mouvement ouvrier organisé est apparu dans le courant du 19ième siècle.
- Ce battre pour le respect des décisions des Cours


YES WE SCAN
YES WE SCAN
YES WE SCAN
YES WE
JESUS DIAZ-FRONT

3. La résistance juridique

- <u>4 arrêts en matière du privacy</u>
- 1. Cour de Justice de l'UE, 8 avril 2014 (C-293/12; C-594-12) annulation directive sur la conservation des données
- 2. Cour de Justice de l'UE, 13 mai 2014 (C-131/12) Mario Costeja Gonzales c. Google Spain
- 3. Cour constitutionelle belge, 11 juin 2015 (5856; 5859) annulation loi belge dataretention
- 4. Cour de Justice de l'UE, 6 octobre 2015 (C-362/14) Max Schrems c. Data Protection Commissioner

1. Cour de Justice de l'UE, 8 avril 2014; annulation directive sur la conservation des données

- Directive 2006/24
- High Court Irlande; Verfassungsrechtshof Autriche
- Incompatible avec les articles 7, 8 eet 52 § 1 Charte des droits fondamentaux de l'UE

- 7: respect de la vie privée et familiale

- 8: protection données à caractère personnel. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification. Le respect de ces règles est soumis au contrôle d'une autorité indépendante.

- 52: Toute limitation de l'exercice des droits et libertés reconnus par la présente Charte doit être prévue par la loi et respecter le contenu essentiel desdits droits et libertés. Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui.

- 5 Eléments

1.

La directive comporte une ingérence d'une vaste ampleur et d'une gravité particulière dans les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel sans que *cette ingérence soit limitée au strict nécessaire.*

- La Cour constate tout d'abord que les données à conserver permettent notamment de savoir (1) avec quelle personne et par quel moyen un abonné ou un utilisateur inscrit a communiqué, (2) de déterminer le temps de la communication ainsi que l'endroit à partir duquel celle-ci a eu lieu et (3) de connaître la fréquence des communications de l'abonné ou de l'utilisateur inscrit avec certaines personnes pendant une période donnée. Ces données, prises dans leur ensemble, sont susceptibles de **fournir des indications très précises sur la vie privée des personnes dont les données sont conservées, comme les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales et les milieux sociaux fréquentés.** (27)

- La Cour estime qu'en imposant la conservation de ces données et en en permettant l'accès aux autorités nationales compétentes, la directive s'immisce de manière particulièrement grave dans les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel. En outre, le fait que la conservation et l'utilisation ultérieure des données sont effectuées sans que l'abonné ou l'utilisateur inscrit en soit informé est **susceptible de générer dans l'esprit des personnes concernées le sentiment que leur vie privée fait l'objet d'une surveillance constante.** (37)

2.

La conservation des données en vue de leur transmission éventuelle aux autorités nationales compétentes **répond effectivement à un objectif d'intérêt général, à savoir la lutte contre la criminalité grave ainsi que, en définitive, la sécurité publique**

3.

Toutefois, la Cour estime qu'en adoptant la directive sur la conservation des données, le législateur de l'Union a excédé les limites qu'impose le respect du principe de proportionnalité.

- Si la conservation des données imposée par la directive peut être considérée comme apte à réaliser l'objectif poursuivi par celle-ci, **l'ingérence vaste et particulièrement grave de cette directive dans les droits fondamentaux en cause n'est pas suffisamment encadrée afin de garantir que cette ingérence soit effectivement limitée au strict nécessaire.**

Trois arguments

premièrement, la directive couvre de manière généralisée l'ensemble des individus, des moyens de communication électronique et des données relatives au trafic sans qu'aucune différenciation, limitation ou exception soit opérée en fonction de l'objectif de lutte contre les infractions graves.

- 52 S'agissant du droit au respect de la vie privée, la protection de ce droit fondamental exige, selon la jurisprudence constante de la Cour, en tout état de cause, que les dérogations à la protection des données à caractère personnel et les limitations de celle-ci doivent s'opérer dans les **limites du strict nécessaire**

- 56 Quant à la question de savoir si l'ingérence que comporte la directive 2006/24 est limitée au strict nécessaire, il convient de relever que cette directive impose, … la conservation de toutes les données relatives au trafic concernant la téléphonie fixe, la téléphonie mobile, l'accès à l'internet, le courrier électronique par Internet ainsi que la téléphonie par l'internet. Ainsi, elle vise tous les moyens de communication électronique dont l'utilisation est très répandue et d'une importance croissante dans la vie quotidienne de chacun. En outre, conformément à son article 3, ladite directive couvre tous les abonnés et utilisateurs inscrits. Elle comporte donc une ingérence dans les droits fondamentaux de la quasi-totalité de la population européenne.

- 57 À cet égard, il importe de constater, en premier lieu, que la directive 2006/24 couvre de manière généralisée toute personne et tous les moyens de communication électronique ainsi que l'ensemble des données relatives au trafic sans qu'aucune différenciation, limitation ni exception soient opérées en fonction de l'objectif de lutte contre les infractions graves.

- 58 En effet, d'une part, la directive 2006/24 **concerne de manière globale l'ensemble des personnes faisant usage de services de communications électroniques, sans toutefois que les personnes dont les données sont conservées se trouvent, même indirectement, dans une situation susceptible de donner lieu à des poursuites pénales. Elle s'applique donc même à des personnes pour lesquelles il n'existe aucun indice de nature à laisser croire que leur comportement puisse avoir un lien, même indirect ou lointain, avec des infractions graves. En outre, elle ne prévoit aucune exception, de sorte qu'elle s'applique même à des personnes dont les communications sont soumises, selon les règles du droit national, au secret professionnel.**

- 59 D’autre part, tout en visant à contribuer à la lutte contre la criminalité grave, ladite directive ne requiert aucune relation entre les données dont la conservation est prévue et une menace pour la sécurité publique et, notamment, elle n’est pas limitée à une conservation portant soit sur des données afférentes à une période temporelle et/ou une zone géographique déterminée et/ou sur un cercle de personnes données susceptibles d’être mêlées d’une manière ou d’une autre à une infraction grave, soit sur des personnes qui pourraient, pour d’autres motifs, contribuer, par la conservation de leurs données, à la prévention, à la détection ou à la poursuite d’infractions graves.

Deuxièmement, la directive ne prévoit aucun critère objectif qui permettrait de garantir que les autorités nationales compétentes n'aient accès aux données et ne puissent les utiliser qu'aux seules fins de prévenir, détecter ou poursuivre pénalement des infractions susceptibles d'être considérées, au regard de l'ampleur et de la gravité de l'ingérence dans les droits fondamentaux en question, comme suffisamment graves pour justifier une telle ingérence. Au contraire, la directive se borne à renvoyer de manière générale aux « infractions graves » définies par chaque État membre dans son droit interne. De plus, la directive ne prévoit pas les conditions matérielles et procédurales dans lesquelles les autorités nationales compétentes peuvent avoir accès aux données et les utiliser ultérieurement. L'accès aux données n'est notamment pas subordonné au contrôle préalable d'une juridiction ou d'une entité administrative indépendante.

60 En deuxième lieu, à cette absence générale de limites s'ajoute le fait que la directive 2006/24 ne prévoit aucun critère objectif permettant de délimiter l'accès des autorités nationales compétentes aux données et leur utilisation ultérieure à des fins de prévention, de détection ou de poursuites pénales concernant des infractions pouvant, au regard de l'ampleur et de la gravité de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte, être considérées comme suffisamment graves pour justifier une telle ingérence.

- 62 En particulier, la directive 2006/24 ne prévoit aucun critère objectif permettant de limiter le nombre de personnes disposant de l'autorisation d'accès et **d'utilisation ultérieure** des données conservées au strict nécessaire au regard de l'objectif poursuivi. Surtout, l'accès aux données conservées par les autorités nationales compétentes n'est pas subordonné à un contrôle préalable effectué soit par une juridiction, soit par une entité administrative indépendante …

Troisièmement, s'agissant de la durée de conservation des données, la directive impose une durée d'au moins six mois sans opérer une quelconque distinction entre les catégories de données en fonction des personnes concernées ou de l'utilité éventuelle des données par rapport à l'objectif poursuivi. (63, 64)

4.

La Cour constate par ailleurs que la directive ne prévoit pas de garanties suffisantes permettant d'assurer une protection efficace des données contre les risques d'abus ainsi que contre l'accès et l'utilisation illicites des données. Elle relève entre autres que la directive autorise les fournisseurs de services à tenir compte de considérations économiques lors de la détermination du niveau de sécurité qu'ils appliquent (notamment en ce qui concerne les coûts de mise en oeuvre des mesures de sécurité) et qu'elle ne garantit pas la destruction irrémédiable des données au terme de leur durée de conservation. (66, 67)

5.

La Cour critique enfin le fait que la directive n'impose pas une conservation des données sur le territoire de l'Union. Ainsi, la directive ne garantit pas pleinement le contrôle du respect des exigences de protection et de sécurité par une autorité indépendante, comme cela est pourtant explicitement exigé par la charte. Or, un tel contrôle, effectué sur la base du droit de l'Union, constitue un élément essentiel du respect de la protection des personnes à l'égard du traitement des données à caractère personnel. (68)

2. Cour de Justice de l'UE, 13 mai 2014 (C-131/12) Mario Costeja Gonzalez, contre Google Spain

- Google Search; 2 pages 1998 La Vanguardia
- L'exploitant d'un moteur de recherche sur Internet est responsable du traitement qu'il effectue des données à caractère personnel qui apparaissent sur des pages web publiées par des tiers.
- Ainsi, lorsque, à la suite d'une recherche effectuée à partir du nom d'une personne, la liste de résultats affiche un lien vers une page web qui contient des informations sur la personne en question, la personne concernée peut s'adresser directement à l'exploitant ou, lorsque celui-ci ne donne pas suite à sa demande, saisir les autorités compétentes pour obtenir, sous certaines conditions, la suppression de ce lien de la liste de résultats

3. Cour constitutionelle belge, 11 juin 2015 (5856; 5859) annulation loi belge dataretention

- **La loi belge du 30 juillet 2013**

- Après 7 ans
- Chambre et Sénat: 22 jours, vacances, pas commissions justice, pas d'experts
- Procedures Cour Constitutionnelle: Ordre des barreaux francophones et germanophone; Ligues des droits de l'homme

- La loi belge ne se limite même pas à la 'criminalité grave' mais parle 'd'infractions pénales'; tous les crimes et délits sont concernés.
- La loi belge prévoit aussi la conservation de ces données pour, et leur accessibilité par, les services de renseignement et de sécurité.
- La loi belge prévoit aussi l'accès à ces données au Service de médiation pour les télécommunications et pour la répression d'appels malveillants vers les services d'urgence.

- B.10.1. Comme la Cour de justice l'a relevé aux points 56 et 57 de son arrêt, la directive impose la conservation de toutes les données relatives au trafic concernant la téléphonie fixe, la téléphonie mobile, l'accès à l'internet, le courrier électronique par internet ainsi que la téléphonie par l'internet, couvrant de manière généralisée toute personne et tous les moyens de communication électronique sans distinction en fonction de l'objectif de lutte contre les infractions graves que le législateur de l'Union entendait poursuivre. La loi attaquée ne se distingue nullement de la directive sur ce point. En effet, ainsi qu'il est dit en B.8, les catégories de données qui doivent être conservées sont identiques à celles énumérées par la directive tandis qu'aucune distinction n'est opérée quant aux personnes concernées ou aux règles particulières à prévoir en fonction de l'objectif de lutte contre les infractions décrites à l'article 126, § 2, de la loi du 13 juin 2005 remplacé par la loi attaquée. Tout comme la Cour de justice l'a constaté à propos de la directive (point 58), la loi s'applique donc également à des personnes pour lesquelles il n'existe aucun indice de nature à laisser croire que leur comportement puisse avoir un lien, même indirect ou lointain, avec les infractions énumérées par la loi attaquée. De même, la loi s'applique sans aucune exception, également à des personnes dont les communications sont soumises au secret professionnel.

- B.10.2. Pas plus que ce n'est le cas pour la directive, l'article 5 attaqué ne requiert-il une relation entre les données dont la conservation est prévue et une menace pour la sécurité publique. Il ne limite pas non plus la conservation des données afférentes à une période temporelle ou à une zone géographique déterminée ou encore à un cercle de personnes susceptibles d'être mêlées à une infraction visée par la loi, ou qui pourraient contribuer par la conservation des données, à prévenir, détecter ou poursuivre ces infractions.

- B.10.3. Si les autorités compétentes pour avoir accès aux données conservées sont énumérées à l'article 126, § 5, 3°, de la loi du 13 juin 2005, remplacé par l'article 5 de la loi attaquée, aucune condition matérielle ou procédurale n'est définie par la loi quant à cet accès.

- B.10.4. Enfin, en ce qui concerne la durée de conservation des données, la loi n'opère aucune distinction entre les catégories de données en fonction de leur utilité éventuelle aux fins de l'objectif poursuivi ou selon les personnes concernées. 34 B.11. **Par identité de motifs avec ceux qui ont amené la Cour de justice de l'Union européenne** à juger la directive « conservation des données » invalide, il y a lieu de constater que par l'adoption de l'article 5 de la loi attaquée, le législateur a excédé les limites qu'impose le respect du principe de proportionnalité au regard des articles 7, 8 et 52 1 de la Charte

4. Cour de Justice de l'UE, 6 octobre 2015 (C-362/14) Max Schrems c. Data Protection Commissioner

- Contre Facebook (conséquences pour 4.410)
- Safe Harbour-système; décision Commission européenne de 2010; transfer data UE vers EUA
- Max Schrems: 2008-2011; 1.222 pages data, aussi data effacés
- 'Mijlpaal voor onze onlineprivacy' (un tournant)
- 'Belangrijke slag toegediend aan de globale surveillance van de VS' (coup important)
- 'Europees Hof maakt duidelijk dat massasurveillance onze fundamentele rechten aantast' (affecte nos droits)

- 22 En outre, au point 7 de cette communication, la Commission a fait état de ce que «toutes les entreprises participant au programme PRISM [programme de collecte de renseignements à grande échelle], qui permettent aux autorités américaines d'avoir accès à des données stockées et traitées aux États-Unis semblent être certifiées dans le cadre de la sphère de sécurité» et que celle-ci «est donc devenue l'une des voies par lesquelles les autorités américaines du renseignement ont accès à la collecte des données à caractère personnel initialement traitées dans l'[Union]». À cet égard, la Commission a constaté, au point 7.1 de ladite communication, «qu'un certain nombre de bases juridiques prévues par la législation américaine permettent la collecte et le traitement à grande échelle des données à caractère personnel stockées ou traitées par des sociétés établies aux États-Unis» et que «[c]es programmes étant à grande échelle, il est possible que les données transférées dans le cadre de la sphère de sécurité soient accessibles aux autorités américaines et traitées par celles-ci au-delà de ce qui est strictement nécessaire et proportionné à la protection de la sécurité nationale, comme le prévoit l'exception énoncée dans la décision [2000/520]».

- 25 La Commission a conclu, à ce même point 8, que «l'accès à grande échelle des agences de renseignement aux données que des entreprises certifiées au titre de la sphère de sécurité transfèrent aux États-Unis soulève de graves questions sur la continuité de la sauvegarde des droits des citoyens européens en matière de protection des données lorsque des données les concernant sont transférées aux États-Unis».

- 81 Si le recours, par un pays tiers, à un système d'autocertification n'est pas, par lui-même, contraire à l'exigence prévue à l'article 25, paragraphe 6, de la directive 95/46, selon laquelle le pays tiers concerné doit assurer un niveau de protection adéquat «en raison de [la] législation interne ou [des] engagements internationaux» de ce pays, la fiabilité d'un tel système, au regard de cette exigence, repose essentiellement sur la mise en place de mécanismes efficaces de détection et de contrôle permettant d'identifier et de sanctionner, en pratique, d'éventuelles violations des règles assurant la protection des droits fondamentaux, notamment du droit au respect de la vie privée ainsi que du droit à la protection des données à caractère personnel.


facebook

Yes we scan

- 82 En l'occurrence, les principes de la sphère de sécurité sont, en vertu de l'annexe I, deuxième alinéa, de la décision 2000/520, «exclusivement destinés aux organisations américaines recevant des données à caractère personnel en provenance de l'Union européenne et doivent permettre à ces organisations de remplir les conditions relatives à la 'sphère de sécurité' de façon à bénéficier de la présomption de 'niveau de protection adéquat' que prévoit celle-ci». Ces principes sont donc uniquement applicables aux organisations américaines autocertifiées recevant des données à caractère personnel depuis l'Union, sans qu'il soit exigé que les autorités publiques américaines soient soumises au respect desdits principes.

- 88 Au surplus, la décision 2000/520 ne comporte aucune constatation quant à l'existence, aux États-Unis, de règles à caractère étatique destinées à limiter les éventuelles ingérences dans les droits fondamentaux des personnes dont les données sont transférées depuis l'Union vers les États-Unis, ingérences que des entités étatiques de ce pays seraient autorisées à pratiquer lorsqu'elles poursuivent des buts légitimes, tels que la sécurité nationale.

- 93 Ainsi, n'est pas limitée au strict nécessaire une réglementation qui autorise de manière généralisée la conservation de l'intégralité des données à caractère personnel de toutes les personnes dont les données ont été transférées depuis l'Union vers les États-Unis sans qu'aucune différenciation, limitation ou exception soit opérée en fonction de l'objectif poursuivi et sans que soit prévu un critère objectif permettant de délimiter l'accès des autorités publiques aux données et leur utilisation ultérieure à des fins précises, strictement restreintes et susceptibles de justifier l'ingérence que comportent tant l'accès que l'utilisation de ces données

- 94 En particulier, une réglementation permettant aux autorités publiques d'accéder de manière généralisée au contenu de communications électroniques doit être considérée comme portant atteinte au contenu essentiel du droit fondamental au respect de la vie privée, tel que garanti par l'article 7 de la Charte (voir, en ce sens, arrêt Digital Rights Ireland e.a., C-293/12 et C-594/12, EU:C:2014:238, point 39).

4. La résistance des citoyens

Respect pour les décisions des Cours

- Réactions arrêt Cour Constitutionnelle

- De Morgen, 12.6.2015: 'Moordenaars krijgen nu vrij spel. Willen we dat?'
- Het Laatste Nieuws, 12.6.2015: 'Verkrachters ….'
- De Standaard, 12.6.2015: Privacy-arrest bezorgt speurders kopzorgen
- Le Soir, 12.6.2015: Victoire des défenseurs de la vie privée
- De Standaard, 26.6.2015: Procureurs-generaal trekken aan alarmbel over dataretentie


NATÚÚRLIJK KAN 'T NIET DAT FACEBOOK DE PRIVACY SCHENDT VAN ONWETENDE BURGERS...
DAT IS DE OVERHEID HAAR TAAK...
LECTRR

Contrer l'avant-projet de la loi relative à la collecte et à la conservation des données dans le secteur des communications électroniques

- Juillet 2013; gouvernement belge (Geens, De Croo, Vandeput)
- -très vite
- -'la conservation des données n'est pas de la surveillance de masse'
- -'limitation disproportionnée' découle de 4 éléments (toutes les personnes; pas de différenciation en fonction de données conservées; insufficance de règles à l'accès; absence ou faiblesse règles sur la sécurisation)
- -réponse: 'Après analyse approfondie, il ressort qu'il n'est pas possible d'opérer une différenciation en fonction des personnes (e.a. certaines professions), périodes temporelles et zones géographiques'; 'Il faut 'compenser' cet élément par un régime plus strict sur les trois autres aspects'
- -certains 'garanties nouveaux' e.a. différenciation de la période de conservation en fonction de données conservées; accès seulement pour crimes peines minimum un an; …

- 4. La conservation des données n'est pas de la surveillance de masse. Il est toutefois essentiel de ne pas confondre cette obligation de conservation avec la surveillance de masse réalisée par certains pays et pour laquelle la presse apporte régulièrement de nouvelles révélations. Cette surveillance est caractérisée par le fait que des services étrangers filtrent et traitent effectivement un nombre gigantesque de données. De La mesure visée par le présent projet de loi ne relève pas du tout de ce type d'approche. Si la conservation touche effectivement tous les citoyens pour autant qu'ils utilisent un téléphone ou Internet, l'accès à et l'utilisation de leurs données seront toujours ciblé et limité à un cas concret pour l'exercice d'une des finalités prévues, en particulier dans le cadre d'une enquête pénale ou de renseignement. Cet accès se fait sous contrôle judiciaire pour l'enquête pénale ou sous contrôle d'une commission indépendante (Commission BIM) pour le renseignement. Les abus sont punissables. Il sera en outre toujours limité dans le temps avec un maximum de 12 mois pour les données d'identification et des délais courts pour les autres données.

- 6. …La Cour conclut que l'article 126 LCE attaqué, comme la directive, constitue une limitation disproportionnée du droit au respect de la vie privée. Cette violation du principe de proportionnalité découle de la combinaison de quatre éléments :
- – Le fait que la conservation des données concerne toutes les personnes ;
- – L'absence de différenciation en fonction des catégories de données conservées et leur utilité ;
- – L'absence ou l'insuffisance de règles quant à l'accès des autorités aux données concernées ;
- – Et enfin, bien que cet élément soit soulevé seulement par la Cour de justice et pas par la Cour constitutionnelle, l'absence ou la faiblesse des règles sur la sécurisation des données chez les fournisseurs ou les opérateurs. Ces éléments, et les réponses que le projet de loi y apporte, sont passés en revue ci-dessous.

- On peut conclure qu'il n'est pas possible de modaliser l'article 126 LCE sur base du premier élément (l'absence de différentiation en fonction des personnes) repris par la Cour constitutionnelle et la Cour de justice. Tous les pays européens contactés sont arrivés à la même conclusion. Ni l'arrêt de la Cour constitutionnelle ni celui de la Cour de justice UE ne concluent toutefois qu'un seul des quatre éléments suffit à constituer une violation du principe de proportionnalité. Si tel était le cas, et l'absence de différenciation entre les personnes constituant **l'élément essentiel** de la législation nationale et européenne annulée, on peut penser que la Cour de justice et la Cour constitutionnelle auraient uniquement examiné cet aspect et auraient conclu à la violation du droit au respect de la vie privée sans examiner les autres éléments.
- Il faut donc combiner les différents éléments soulevés par la Cour de justice UE et la Cour constitutionnelle. Puisque le principe de la conservation généralisée (c'est-à-dire sans différenciation entre les personnes) des données de communication constitue en soi une limitation très importante du droit au respect de la vie privée, il faut « compenser » cet élément par un régime plus strict sur les autres aspects.

- 8. La différenciation en fonction des catégories de données La Cour constitutionnelle note que « […] en ce qui concerne la durée de conservation des données, la loi n'opère aucune distinction entre les catégories de données en fonction de leur utilité éventuelle aux fins de l'objectif poursuivi ou selon les personnes concernées ». Toutes les données faisant l'objet de l'obligation de conservation sont en effet conservées pour une durée unique de 12 mois dans la loi annulée. Le présent projet de loi comble cette lacune et introduit une distinction sur base de 4 catégories de données.. La première catégorie concerne les données d'identification (qui est titulaire de tel numéro de gsm, quel est le numéro de gsm de telle personne, qui se trouve derrière telle adresse IP, …). Ces données, qui sont les plus demandées et sont modérément attentatoires à la vie privée, par rapport notamment aux troisième et quatrième catégories, devront être conservées pour une durée maximale de 12 mois. La deuxième catégorie concerne les données relatives aux services de communication (par exemple les volumes consommés). Ces données étant d'une utilité moindre que les autres catégories, il est normal d'imposer une conservation plus limitée. Elles devront être conservées pendant 2 mois maximum. La troisième catégorie et la quatrième catégories sont interdépendantes et sont traitées ensemble. La troisième catégorie concerne les données de connexion et localisation (quel est notamment le lieu et la durée d'une communication). La quatrième catégorie concerne les données personnelles de communications (qui a appelé ou correspondu avec qui). Les troisième et quatrième catégories sont plus attentatoires à la vie privée que les deux autres. Les accès à ces données sont moins nombreux que ceux aux données d'identification mais restent fréquents. Ces données devront être conservées [9 /12] mois.

- 9. Le renforcement des garanties au niveau de l'accès des autorités aux données. La directive UE a été considérée comme particulièrement problématique parce qu'elle ne réglait que l'obligation de conservation sans réglementer et donc sans encadrer l'accès des autorités aux données concernées. La Cour constitutionnelle note que « si les autorités compétentes pour avoir accès aux données conservées sont énumérées à l'article 126, § 5, 3°, de la loi du 13 juin 2005, remplacé par l'article 5 de la loi attaquée, aucune condition matérielle ou procédurale n'est définie par la loi quant à cet accès. » L'article 126 LCE annulé renvoyait pourtant explicitement, pour les deux régimes d'accès principaux, aux règles régissant cet accès, c'est-à- dire les articles 46bis et 88bis du Code d'instruction criminelle pour le cadre pénal et les articles 18/6 et 18/7 de la Loi organique des services de renseignement et de sécurité pour les accès au niveau de l'activité de renseignement. Le présent projet de loi donne suite à cette partie de l'arrêt de la Cour constitutionnelle en renforçant le lien entre l'article 126 LCE et le régime d'accès défini dans les autres lois précitées. Il clarifie aussi le fait que l'accès aux données conservées n'est possible que pour les finalités explicitement énumérées dans l'article 126 LCE. Mais le présent projet de loi va plus loin en renforçant les garanties prévues par le Code d'instruction criminelle et la Loi organique des services de renseignement et de sécurité. Il encadre aussi mieux l'accès pour les autres finalités. Celles-ci sont précisées et étendues à certaines situations très spécifiques.

- 10. Le renforcement de la sécurisation des données conservées par les opérateurs. Enfin, le projet de loi, faisant suite notamment aux préoccupations émises par la Cour de justice, renforce les mesures à prendre par les opérateurs et fournisseurs de manière à protéger et sécuriser les données et l'accès à celles-ci. Il s'agit notamment de prendre des mesures de protection technologiques à l'égard de ces données, d'assurer la traçabilité des accès, de détruire les données à l'expiration du délai, ou encore de désigner un préposé à la protection des données chargé de veiller au respect des différentes règles en la matière.


WATCHING YOU