Étude comparative sur les différentes approches des nouveaux défis en matière de protection de la vie privée, en particulier à la lumière des évolutions technologiques
Rapport final

Note de synthèse

I. Objet de l’étude

Cette étude avait pour objet d’identifier les défis liés à la protection des données à caractère personnel résultant de phénomènes sociaux et techniques actuels, tels que l’Internet, la mondialisation, l’ omniprésence croissante des données à caractère personnel. Elle a abordé également de la collecte de ces données, la puissance et la capacités accrues des ordinateurs et autres dispositifs de traitement des données, les nouvelles technologies spéciales (telles que la RFID, la biométrie, la reconnaissance faciale, la surveillance accrue - et la «dataveillance»), et l’utilisation accrue des données à caractère personnel à des fins autres que celles auxquelles elles ont été collectées, en particulier dans le cadre de la sécurité nationale et de la lutte contre le crime organisé et le terrorisme. L’étude a de même élaboré un rapport qui dresse une analyse comparative des solutions à ces défis proposées par les différents systèmes réglementaires et non réglementaires (au sein et en dehors de l’UE) et qui tente de déterminer si le cadre juridique de la principale directive CE relative à la protection des données (directive 95/46/CE) offre toujours une protection appropriée ou s’il y a lieu d’envisager de le modifier à la lumière des solutions jugées les plus efficaces.

Cette étude couvre les pays et territoires suivants: l’Allemagne, le Danemark, la France, la Grèce, la République tchèque et le Royaume-Uni; et en dehors de l’Europe, les États-Unis (niveau fédéral, Californie et New Jersey), l’Australie, Hong Kong, l’Inde et le Japon.

II. Les défis

Compte tenu de la chute des coûts liés au stockage, à la transmission et au traitement des données à caractère personnel, les concepteurs des systèmes ont de moins en moins de raisons technologiques et économiques de minimiser la collecte de ces données. Les technologies «Web 2.0» permettent aux utilisateurs de partager des informations (souvent sensibles) les concernant, et concernant leur entourage, comme jamais auparavant. Des étiquettes RFID lisibles à distance sont souvent placées sur les produits de consommation, et des étiquettes semblables sont placées sur les passeports de nombreux pays et sont également utilisées dans les systèmes de péage routier, les billets des transports publics, la gestion des livres dans les bibliothèques et pour de nouvelles cartes de crédit sans contact telles que les cartes «PayPass» de MasterCard et «Paywave» de Visa. Les caméras de télévision en circuit fermé prolifèrent dans les zones urbaines et sur les routes, et permettent une reconnaissance automatique des plaques d’immatriculation des véhicules. La biométrie, et notamment les images faciales et les scanners de l’iris, sont de plus en plus utilisés pour identifier les individus. En outre, toutes ces informations peuvent être transférées à faible coût aux quatre coins du monde, et reproduites dans toutes les bases de données et dans tous les appareils informatiques portables. Il sera de plus en plus difficile d’anonymiser les données. Ces avancées technologiques provoqueront un véritable «raz de marée» numérique de données personnelles, auxquelles il sera possible d’accéder à des fins de surveillance et de marketing et qui pourront être utilisées pour exercer un contrôle sur les individus.

La puissance du traitement ne cessant d’augmenter, il est aujourd’hui possible d’extraire une plus grande quantité d’informations de cette masse de données en utilisant des algorithmes d’extraction pour déterminer des schémas comportementaux et créer des «profils» qui, à leur tour, influencent la façon dont les individus sont traités. Les craintes du public concernant le
terrorisme ont conduit les gouvernements à mettre en commun et à analyser les données relatives aux déplacements, à la situation financière et aux communications des individus. Les systèmes d’administration en ligne, dont l’objectif premier est d’améliorer les services publics tout en réduisant les frais généraux, utilisent souvent des bases de données à l’échelle de la population qui contiennent des données à caractère personnel sensibles sur des millions de personnes. Ces données sont régulièrement interconnectées, analysées et «extraîttes» à des fins administratives, au détriment du contrôle démocratique et de leur contrôle par la personne concernée. De plus en plus souvent, «l’ordinateur» prend des décisions qui ont un «impact significatif» sur les individus, à partir d’algorithmes créés de façon dynamique que même les responsables ou le personnel mettant en œuvre ces décisions ne comprennent pas, et que les personnes concernées n’ont aucun moyen de contester. Protéger les données, ce n’est pas (seulement) protéger la vie privée: c’est aussi contrer les menaces pour les valeurs fondamentales européennes, de plus en plus nombreuses.

L’efficacité de la protection des données dépend donc désormais de la fermeté avec laquelle sont appliqués les principes tels que la limitation de la finalité et la minimisation de la collecte de données à caractère personnel dès la phase de conception des systèmes d’information; et d’un examen approfondi de la proportionnalité des bases de données et des programmes de surveillance du secteur public et du secteur privé.

III/IV. Impératifs fondamentaux et approche de base

Toute révision du régime européen de protection des données doit commencer par la reconnaissance explicite de la nécessité de respecter les prescriptions de la CEDH et de la Charte des droits fondamentaux, ainsi que des Constitutions des États membres. Le non-respect de ces obligations mettra en péril les valeurs constitutionnelles européennes de base et constituera une violation des principes généraux du droit européen, et remettra en question l’acceptation de la suprématie (ou primauté) du droit de la CE et de l’UE par les tribunaux constitutionnels de plusieurs États membres. Les principes, règles et critères européens de protection des données font partie de cette structure des Droits de l’Homme fondamentaux, et ont résisté au passage du temps, même s’ils ont besoin d’être consolidés à certains égards.

Toutefois, leur application et leur exécution n’ont été pas été aussi probantes, et les nouvelles évolutions technologiques risquent de rendre plus difficile encore l’application de ces principes (bien que certaines de ces nouvelles technologies puissent en réalité la faciliter).

La législation européenne en matière de protection des données (dans tous les domaines couverts par les trois anciens piliers) peut et doit continuer de s’appuyer sur les principes et les critères de base de la protection des données définis dans la directive 95/46/CE. L’application de ces normes générales doit être clarifiée mais les normes en elles-mêmes ne nécessitent pas de révision majeure pour faire face aux nouveaux défis. Au contraire, elles reflètent des normes européennes et nationales en matière de droits constitutionnels/de l’Homme du type que nous venons d’évoquer, qui doivent être réaffirmées avec force.
V. Recommandations (uniquement)

L’étude a épinglé différentes questions qu’il conviendra de prendre en compte lors de la révision du régime européen de protection des données, et a formulé à ce sujet les recommandations ci-après (les références entre parenthèses renvoient à la partie V du rapport final, où ces questions sont examinées en détail):

✓ Exclusion problématique de certains domaines du champ d’application de la directive (V.2):

(i) Domaines couverts par les anciens premier et troisième piliers:

Recommandation: Les principes, règles et critères de base en matière de protection des données consacrés dans la directive doivent s’appliquer «de façon uniforme» aux activités appartenant à tous les domaines autrefois couverts par les différents piliers. Il s’agit notamment de l’application des exceptions (limitées) pour les activités du troisième pilier énumérées à l’article 13 de la directive. Si nous voulons pouvoir relever les défis, nous devons renforcer l’harmonisation, ou tout au moins le rapprochement, des règles de protection des données qui régissent ces activités dans l’UE, sur la base de la recommandation R(87)15 du COE. Il est également primordial de garantir une protection judiciaire totale dans les tribunaux nationaux, et par le biais de la CEJ, et de reconnaître pleinement le statut des personnes concernées (avec comme garantie la Cour européenne des Droits de l’Homme).

(ii) Exceptions concernant le traitement des données à des fins exclusivement personnelles et la liberté d’expression, en particulier pour ce qui concerne les sites de réseaux sociaux et le «blogage» sur le «Web 2.0»:

Recommandation: Il devrait être possible d’appliquer les règles de protection des données de façon plus souple aux activités relativement courantes sur l’Internet. Nous pensons que la meilleure façon de résoudre ce problème consiste à réglementer les services qu’utilisent ces utilisateurs, en particulier les sites de réseaux sociaux. Les entreprises devraient être contraintes de doter leurs sites et leurs services de paramètres par défaut et d’outils respectueux de la vie privée: si les paramètres par défaut ne protègent pas la vie privée et les données à caractère personnel, le site qui a défini ces paramètres doit en assumer la responsabilité principale. Cela laisserait la possibilité d’adopter un régime (ou, s’il existe déjà, de le conserver) de délits et quasi-délits [quasi-délit ou faute] en vertu duquel les individus peuvent être tenus pour responsables de divulgation publique abusive ou injustifiée d’informations à caractère privé ou d’«intrusion», sur l’Internet.

✓ La question délicate du «droit applicable» (V.3)

Recommandation: Il est absolument indispensable d’améliorer, de clarifier et de préciser les règles relatives au droit applicable. Nous proposons quelques pistes à suivre pour améliorer ces règles (voir le texte intégral du rapport final pour les oppositions à ces suggestions):
Note de synthèse

– Au sein de l’UE/EEE, les règles devraient, à notre avis, être simplement fondées sur le principe du « pays d’origine », comme cela devait être initialement le cas. Il est toutefois essentiel d’assurer une plus grande harmonisation, ou du moins un rapprochement à haut niveau, entre les législations des États membres (voir ci-dessous).

– Les entreprises qui n’appartiennent pas à l’UE/EEE et qui sont « établies » dans l’UE/EEE devraient pouvoir se conformer uniquement à la législation du pays UE/EEE où se situe leur principal établissement (leur QG européen) et, sinon, devraient être traitées comme des entreprises UE/EEE.

– Pour les entreprises non membres de l’UE/EEE qui ne sont pas « établies » dans l’UE/EEE mais qui utilisent des « moyens » dans l’UE/EEE (généralement des entreprises qui n’appartiennent pas à l’UE/EEE et qui offrent leurs produits ou services à des citoyens et entreprises appartenant à l’UE/EEE via l’Internet), les règles relatives au « droit applicable » devraient être simplifiées de manière qu’elles puissent, elles aussi, ne se conformer qu’à la loi d’un seul pays membre (pertinent) de l’UE/EEE. Il pourrait être envisagé de rendre ce choix de législation possible dans le cadre des règles d’entreprise contraignantes; le caractère approprié du choix de législation serait l’un des éléments à prendre en compte pour juger du caractère adéquat et approprié des règles d’entreprise contraignantes.

– Les entreprises qui n’appartiennent pas à l’UE/EEE et qui sont soumises à une législation offrant une protection « adéquate » dans leur pays (selon ce qui aura été déterminé par la Commission) devraient être traitées de la même façon que les entreprises qui appartiennent à l’UE/EEE, c’est-à-dire qu’elles devraient pouvoir ne se conformer qu’à leur propre législation (« adéquate ») – à condition que les États concernés se conforment également aux mesures prises dans l’UE/EEE pour garantir une application harmonisée/comparable de la législation.

✓ La nécessité d’une harmonisation beaucoup plus large (à haut niveau) au sein de l’UE/EEA par différents moyens, y compris le renforcement des mesures d’application par la Commission (V.4)

Remarque : L’étude examine en détail les différences entre les législations des différents États membres pour plusieurs questions importantes, notamment : concepts et définitions de base (V.4.A(i)), les principes (V.4.A(ii)) et les critères (V.4.A(iii)) de protection des données; le traitement des données sensibles (V.4.A(iv)); les règles relatives aux flux de données transfrontaliers (V.4.A(v)); et les législations des pays non membres de l’UE/EEA dans ces domaines (V.4.B). Les conclusions se trouvent à la partie V, section 4; les informations détaillées dans le Document de travail No. 2. La conclusion générale est que des différences majeures subsistent dans tous ces domaines.

Recommandations : Nous ne recommandons pas de remplacer la directive par un règlement ou par une toute nouvelle directive rédigée en des termes beaucoup plus stricts. Nous recommandons plutôt de demander au WP29, en consultation avec la Commission (qui, de toute façon, lui sert de secrétariat) de multiplier et d’approfondir ses études sur les législations et pratiques nationales afin de définir les « meilleures pratiques » et de proposer des interprétations (ce qu’il fait déjà), tout en demandant aussi aux États membres d’expliquer dans quelle mesure ils adhèrent (ou estiment qu’ils ne devraient pas être obligés d’adhérer) à
ces suggestions. Il appartiendrait ensuite à la Commission, le cas échéant, de vérifier si les directives du WP29 sont celles qui, dans le droit, doivent être suivies par les États membres - en considérant les mesures d’exécution forcée comme une façon normale de vérifier cela si nécessaire. Nous pensons que cette solution ne nécessiterait aucune modification de la directive. Elle témoignerait néanmoins d’un changement radical dans l’approche de la Commission vis-à-vis de l’harmonisation de la transposition et de la mise en œuvre des directives puisque les avis du WP29 seraient effectivement mis en application, le cas échéant, par la Commission (sous la supervision, bien entendu, de la CJE).

Pour faire un premier pas dans cette direction, et afin de permettre au WP29 et à la Commission d’agir, nous recommandons que les positions du WP29 ainsi que les informations relatives à leur transposition dans les législations et pratiques nationales des États membres soient présentées de façon plus structurée et plus complète, et que l’attention des organismes administratifs et judiciaires compétents aux niveaux national et européen soit attirée sur ces informations.

La nécessité d’un renforcement de la coopération avec les pays non membres de l’UE, et d’une plus grande reconnaissance des efforts des pays non membres concernant le caractère «adéquat» (V.5)

Recommandation: Le processus de constatation du «caractère adéquat» n’a pas (encore?) eu l’impact qu’il aurait pu avoir, et doit être revu. La prise de décisions provisoires est une piste qui pourrait être explorée. Quoiqu’il en soit, il est indispensable de maintenir et de soutenir fermement les autres mesures, moins formelles, telles que l’assistance technique, la collaboration étroite (y compris les «jumelages» de DPA européennes et non européennes) et les autres processus. En attendant, il est important, au niveau politique, de faire en sorte que le processus de l’article 25 de la directive ne perde pas l’impact qu’il pourrait avoir au niveau international.

La nécessité d’assurer une plus grande conformité avec la législation existante et de renforcer sa mise en application, au niveau national, par les DPA (V.6).

Recommandations: Nous recommandons une «vérification préalable» de tous les systèmes d’information à l’échelle de la population dans l’État membre, en particulier dans le secteur public - mais (i) avant qu’ils ne soient définitifs (c’est-à-dire dès le début de la phase de planification) et (ii) par un personnel plus qualifié (du point de vue technique). Il est intéressant de constater que le Gouvernement australien a récemment proposé que soit conféré au Commissaire à la vie privée du pays le pouvoir de demander aux agences gouvernementales de préparer des évaluations des facteurs relatifs à la vie privée. Dans le secteur privé, les audits en matière de protection de la vie privée ou les labels de protection de la vie privée (réels et efficaces) pourraient jouer un rôle similaire, étant fortement encouragés par des règles relatives aux marchés publics conférant un avantage concurrentiel aux produits et services respectueux de la protection des données (comme cela est déjà le cas en Allemagne, dans le Land du Schleswig-Holstein) (voir ci-dessous). De manière plus générale, nous pensons qu’il pourrait être envisagé de retirer en grande partie le pouvoir de mise en application des mains des DPA pour le placer dans celles des tribunaux et des autorités chargées des poursuites.
La nécessité de renforcer les droits et les voies de recours des particuliers (pouvant agir en collaboration avec ou par l’intermédiaire d’ONG compétentes) (V.7)

Recommandations: Les conditions de base à remplir pour rendre réellement efficace le «recours juridictionnel» prévu à l’article 22, doivent être débattues au sein du WP29, et des directives doivent être formulées à ce sujet - et la Commission doit prendre des mesures d’exécution forcée en cas de non-respect de ces conditions. Une étude devrait être entreprise afin d’examiner les différentes façons d’aider les particuliers à cet égard, par exemple en modifiant les règles relatives au coût des poursuites; en autorisant les groupes non gouvernementaux/de la société civile à contribuer ou à participer officiellement aux poursuites engagées par des particuliers, ou à agir au nom de groupes de personnes concernées; en accordant, par défaut, des dommages-intérêts conventionnels; ou en adoptant des systèmes spéciaux tels que la procédure de «qui tam» aux États-Unis.

La nécessité de développer les mesures supplémentaires et alternatives (tout en comprenant les limites intrinsèques de ces mesures et leurs restrictions pratiques) (V.8)

Remarque: L’étude a examiné en détail les avantages potentiels et les limites – ainsi que les promesses souvent illusoires ou non tenues - des Technologies renforçant la protection de la vie privée (PET), y compris le cryptage (comme moyen d’assurer la conformité au moins avec les obligations en matière de sécurité des données) et une question connexe: la notification des infractions à la sécurité; la désidentification; et d’autres éléments, tels que la P3P et les systèmes d’accès en ligne pour les personnes concernées; la Gestion des identités respectueuse de la vie privée, y compris les systèmes centralisés (aujourd’hui largement dépassés), les systèmes plus récents centrés sur l’utilisateur, les systèmes de gestion des données centrés sur le client («vendor relationship management systems»), et l’utilisation des cartes d’identités à des fins diverses; la prise en compte du respect de la vie privée (Privacy by Design), y compris l’utilisation des évaluations des facteurs liés à la vie privée (Privacy Impact Assessments); les contrôles de la vie privée par les utilisateurs et les paramètres par défaut; l’autoréglementation et la coréglementation sectorielles; et les labels de protection de la vie privée. Nous nous contenterons ici de livrer nos conclusions générales.

Recommandation: Toute révision des mesures complémentaires et alternatives doit être fondée sur une évaluation réaliste et techniquement correcte de ces mesures. Cela ne veut pas dire qu’elles doivent être rejetées d’emblée. Elles devront toutefois être soumises à un examen minutieux par des experts techniques et juridiques.

Il pourrait en effet être utile d’envisager la création d’un organisme ou d’un bureau spécial regroupant les DPA de l’UE/EEE, qui travaillerait en étroite collaboration avec le WP29 et la Commission et qui serait chargé du Label européen de protection des données personnelles, des codes de déontologie européens, et des règles d’entreprise contraignantes, sur une base quasi-commerciale (ou au moins sur la base d’un autofinancement) de façon très similaire au système du Schleswig-Holstein.

De manière générale, la question des incitations et de l’aspect économique de la protection de la vie privée et de la sécurité des données est une question centrale. Si la loi rend économiquement attrayante la protection de la vie privée (par exemple, via des incitations en termes d’approvisionnement, associées à la délivrance de labels sérieux de protection de la vie privée), ou si elle punit les violations des règles en matière de protection et de sécurité des données (en attribuant la responsabilité de la protection à ceux qui sont le mieux placés pour
la garantir plutôt qu’en les autorisant à en faire assumer le coût par les autres, par exemple les consommateurs), alors la protection des données a peut-être un avenir. Nous pensons que cela demande une combinaison harmonieuse de lois et de règles et mécanismes d’autoréglementation. Nous espérons que les considérations ci-dessus susciteront une réflexion à ce sujet.

-o-O-o-

Experts principaux:
Prof. Douwe Korff (R-U/Pays-Bas)
Dr Ian Brown (R-U)

Experts spéciaux:
Prof. Peter Blume (Danemark)
Prof. Graham Greenleaf (Australie)
Prof. Chris Hoofnagle (États-Unis)
Prof. Lilian Mitrou (Grèce)
Filip Pospíšil, Helena Svatošová,
et Marek Tichy (République tchèque)

Conseillers:
Prof. Ross Anderson (R-U)
Caspar Bowden (R-U/France)
Prof. Katrin Nyman-Metcalf (Estonie)
Paul Whitehouse (R-U)