Protection des données à caractère personnel: traitement des données à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et libre circulation des données

2012/0010(COD) - 27/04/2016 - Acte final

OBJECTIF : garantir l'efficacité de la coopération judiciaire en matière pénale et de la coopération policière et faciliter l'échange de données à caractère personnel entre les autorités compétentes des États membres, tout en assurant un niveau élevé et homogène de protection des données à caractère personnel des personnes physiques (réforme de la protection des données).

ACTE LÉGISLATIF : Directive (UE) 2016/680 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil.

CONTENU : la nouvelle directive vise à protéger les données à caractère personnel traitées à des fins de prévention et de détection des infractions pénales, d'enquêtes ou de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces. Elle répond à la nécessité garantir un niveau élevé et systématique de protection des données à caractère personnel des personnes physiques tout en facilitant en parallèle l'échange de ces données entre les services répressifs des différents États membres.

La réforme de la protection des données comprend également un nouveau règlement général sur la protection des données (destiné à remplacer la directive 95/46/CE).

Les principaux éléments de la directive sont les suivants :

Champ dapplication : la directive s'applique au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier. Elle s'applique aussi bien au traitement transfrontière des données à caractère personnel qu'au traitement de ce type de données par les autorités policières et judiciaires au niveau national.

Le directive sapplique non seulement aux autorités publiques compétentes, mais aussi aux organismes ou entités auxquels le droit d'un État membre confie l'exercice de l'autorité publique et des prérogatives de puissance publique à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales.

Principes relatifs aux données à caractère personnel : les États membres doivent prévoir que les données à caractère personnel seront :

- traitées de manière licite, loyale et transparente au regard de la personne concernée,
- collectées pour des finalités déterminées, explicites et légitimes et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités ;
- adéquates, pertinentes et limitées à ce qui est nécessaire pour les finalités pour lesquelles elles sont traitées ;
- conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées ;
- traitées de façon à garantir une sécurité des données, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle.

Traitement ultérieur : la directive prévoit que le traitement des données, par le même responsable du traitement ou un autre, pour l'une des finalités énoncées à la directive, autre que celle pour laquelle les données à caractère personnel ont été collectées, n'est permis que lorsque le responsable du traitement est autorisé à traiter ces données pour une telle finalité conformément au droit de l'Union ou au droit d'un État membre et que le traitement est nécessaire et proportionné à cette autre finalité.

Délais de conservation et d'examen : les États membres doivent prévoir que des délais sont fixés pour l'effacement des données à caractère personnel ou pour la vérification régulière de la nécessité de conserver ces données. Des règles procédurales doivent garantir le respect de ces délais.

Catégories de personnes concernées : les États membres doivent permettre au responsable du traitement d'établir une distinction claire, le cas échéant et dans la mesure du possible, entre les données à caractère personnel de différentes catégories de personnes concernées.

Licéité du traitement des données : un traitement ne sera licite que sil est nécessaire à l'exécution d'une mission effectuée par une autorité compétente, pour les finalités énoncées à la directive, et où il est fondé sur le droit de l'Union ou le droit d'un État membre.

Le traitement des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, ou l'appartenance syndicale, et le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sera autorisé uniquement en cas de nécessité absolue, sous réserve de garanties appropriées pour les droits et libertés de la personne concernée.

Toute décision fondée exclusivement sur un traitement automatisé, y compris le profilage, qui produit des effets juridiques défavorables pour la personne concernée sera interdite, sauf si le droit de l'Union ou le droit d'un État membre l'autorise et si des garanties applicables aux droits et aux libertés de la personne concernée sont fournies.

Droits de la personne concernée : les nouvelles règles comprennent :

- le droit de la personne dêtre informée, en des termes clairs et simples, que des données la concernant sont en cours de traitement ;
- le droit de la personne concernée dêtre informée sur l'identité et les coordonnées du responsable du traitement et sur les finalités du traitement ;
- le droit daccès aux données à caractère personnel et dêtre informé des motifs du refus daccès à ces informations ;
- le droit d'obtenir la rectification ou l'effacement des données à caractère personnel la concernant ou la limitation de leur traitement.

Responsable du traitement et sous-traitant : le directive établit le cadre juridique régissant la responsabilité concernant tout traitement effectué par un responsable du traitement ou, pour son compte, par un sous-traitant. Le responsable du traitement sera tenu de mettre en uvre des mesures techniques et organisationnelles appropriées et d'être en mesure de démontrer la conformité de ses opérations de traitement avec la directive.

La nouvelle directive prévoit que le responsable du traitement désignera un délégué à la protection des données pour aider les autorités compétentes à faire respecter les règles en matière de protection des données.

Analyse dimpact : l'analyse d'impact constitue un outil permettant d'assurer le respect des dispositions. Lorsqu'un type de traitement est susceptible de présenter un risque élevé pour les droits et libertés des personnes physiques, les autorités compétentes devront procéder à une analyse de l'impact potentiel dudit traitement, en particulier en cas de recours à une nouvelle technologie.

Le responsable du traitement ou le sous-traitant devra consulter l'autorité de contrôle préalablement au traitement des données à caractère personnel qui fera partie d'un nouveau fichier à créer lorsqu'une analyse d'impact indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque.

Transferts de données en dehors de lUE : les nouvelles règles couvrent aussi le transfert de données à caractère personnel vers des pays tiers et des organisations internationales. Ce transfert pourra avoir lieu lorsque la Commission a constaté par voie de décision que le pays tiers ou l'organisation internationale en question assure un niveau de protection adéquat. Lorsqu'elle évalue le caractère adéquat du niveau de protection, la Commission tiendra compte en particulier des éléments tels que l'état de droit, le respect des droits de l'homme et des libertés fondamentales, ainsi que de lexistence d'une ou de plusieurs autorités de contrôle indépendantes dans le pays tiers.

En cas de transmission de données provenant d'un autre État membre, celui-ci devra avoir préalablement autorisé ce transfert. Les transferts effectués sans l'autorisation préalable d'un autre État membre seront autorisés uniquement lorsque le transfert est nécessaire pour prévenir une menace grave et immédiate pour la sécurité publique d'un État membre ou d'un pays tiers ou pour les intérêts essentiels d'un État membre et si l'autorisation préalable ne peut pas être obtenue en temps utile.

Autorités de contrôle : afin de garantir le respect des dispositions du projet de directive, des autorités de contrôle seront chargées de surveiller l'application de la directive.

Voies de recours, responsabilité : la nouvelle directive donne également le droit aux personnes concernées le droit de former un recours juridictionnel effectif contre une décision juridiquement contraignante d'une autorité de contrôle qui la concerne et d'obtenir une compensation si elles subissent un préjudice du fait d'un traitement ne respectant pas les règles.

ENTRÉE EN VIGUEUR : 5.5.2016.

TRANSPOSITION : au plus tard le 6.5.2018. Un État membre peut prévoir que, à titre exceptionnel, les systèmes de traitement automatisé installés avant le 6.5.2016 sont mis en conformité avec l'article 25, paragraphe 1 (journalisation de certaines opérations de traitement dans des systèmes de traitement automatisé), au plus tard le 6 mai 2023.