Article : RGPD – Le virus et l'application digitale

1Illustration G. Doré / Pannemaker

« *Ils ne mouraient pas tous, mais tous étaient frappés* »[1].C'est par cet habile poème que le fabuliste Jean de La Fontaine expose ce thème de l'épidémie de peste qui sévit en France entre 1629 et 1631. Il est à noter qu'à l'époque un bureau de santé a été institué : « *Des médecins et chirurgiens de peste » apparaissent, rémunérés par ces bureaux de santé et se distinguent facilement : ils portent un bâton de couleur, sont revêtu d'un manteau noir, la tête recouverte d'un capuchon empli de plantes odorantes destinées à les protéger des miasmes.* »[2] Si les méthodes de protection laissent un peu à désirer, le port de « masque » semble, à l'époque, être un moyen de se protéger et d'éviter la contamination.

L'épidémie du Covid-19 de ce printemps 2020 a généré une crise sanitaire qui étend ses effets non seulement sur le traitement des données de santé, donnée à caractère personnel de catégorie spéciale mais aussi sur le traitement de données de localisation d'utilisateurs d'appareils nomades afin d'endiguer la contamination.

Quelques pistages actualisés…

En chine[3], un système de QR code coloré via une application disponible depuis février 2020, permet aux personnes « saines » confinées de sortir et de se déplacer pour vaquer à leur occupations :

- Vert :déplacement autorisé
- Jaune : 7 jour de quarantaine
- Rouge 14 jours de quarantaine

Officiellement, ce système se base sur 3 critères :

- Historique de déplacement
- Durée dans une zone de confinement strict
- Relation avec des personnes susceptibles d'être positive

Les personnes s'enregistrent sur Alipay[4] via la plateforme gouvernementale de la province via un formulaire en ligne (*nom ,d'identification nationale, n° de téléphone*) et répondent à un questionnaire sur leurs déplacements et leur état de santé. A partir de cette collecte , le gouvernement local envoie les données pour traitement à une série de sous-traitants (*ex. agences de big Data, operateur TELECOM, agence de santé ,etc*) et pour évaluer le statut de chaque utilisateur enregistré.

Cet applicatif ne présentent pas de garanties suffisantes concernant la protection des données telle qu'appliquée en Europe :

- Le principe de transparence est faible : l'information délivrée se borne à expliquer comment fonctionne l'application ;
- Le principe de licéité n'est que partiellement respecté : la base légale est floue et oscille entre l'intérêt public et une obligation légale. Il n'y a visiblement pas de recueil de consentement ;
- La sécurité n'est pas suffisante :
  - les données sont collectées par le gouvernement local au travers d'Alipay et sont transmises à des opérateurs de big data pour analyse des flux de données et croisement de résultats
  - comment s'effectue la sélection des sous-traitants ?
  - Quid en cas de violations de données ?
- L'exercice des droits des personnes concernées sont inexistants.

[1] Les animaux malades de la peste, J. De La Fontaine,

[2] Voir Les grandes épidémies en France

[3] Voir article Beijing rolls out colour-coded QR system for coronavirus tracking despite concerns over privacy, inaccurate ratings, et , China's QR health code system brings relief for some… and new problems, South China Morning post, Chine

[4] Alipay est un service de paiement en ligne et mobile du groupe Alibaba.

Article : RGPD – Le virus et l'application digitale

Depuis début avril 2020,l'institut Robert Koch a mis au point avec le concours de Thryve (mHealth Pioneers GmbH) une application[5] téléchargeable sur bracelets de remise en forme ou montres connectées. Selon l'institut, l'applicatif répond aux exigences suivantes :

- Collecte du consentement de l'utilisateur pour la finalité annoncée de *« à l'analyse des données scientifiques* ».
- Finalité : *« évaluer la situation actuelle et de mieux estimer le nombre possible non divulgué d'infections à coronavirus à l'aide de données provenant de bracelets de fitness* » ;
- Transmission via des destinataires : Google Fit, Apple Health (app) , Fitbit, Garmin, Polar et Withings / Nokia (appareils) ;
- Mesures de sécurité : pseudonymisation[6].

L'Allemagne est ainsi le 1ier pays européen à mettre en œuvre le « *e-tracking* » de ses citoyens moyennant le consentement préalable. Cependant , les exigences suivantes ne sont pas satisfaites :

- Les garanties de sécurité suffisantes de transmission entre les destinataires ;
- Les transfert de données personnelles hors de l'union européenne sachant que certains destinataires ont leurs datacenters hors Europe (*ex. Google, Apple*). L'information concernant l'adéquation au privacy Shield de ces destinataires serait utile ;
- La durée de conservation des données et leur formes pour usage statistique.

Préambule

Le Comité Européen de la Protection des Données (CEPD) a publié, ce 19 mars 2020, une déclaration[7] relative aux traitements des données personnelles dans le contexte cette crise sanitaire.

Pour rappel, l'art 9 du Règlement Général de Protection des Données (*ci-après « RGPD »*) liste les données personnelles de catégorie spéciale parmi lesquelles « *des données concernant la santé* » et en interdit le traitement à moins d'être dans le cas d'une des 10 exemptions. Néanmoins l'utilisation de données de santé *« par un professionnel de la santé soumis à une obligation de secret professionnel* »[8] reste possible. Les états -membres de l'union Européenne ont la latitude d'introduire des conditions supplémentaires et de permettre par exemple, le recours à des système de localisation des individus pour autant que les données soient anonymisées et dans des **finalités très spécifiques** :

1. la notion de régime dérogatoire [9] dans le cadre de la santé et notamment à des fins de :
   - Alerte sanitaire ;
   - Prévention ou de contrôle de maladies transmissibles ;
   - Autres menaces graves pour la santé.

2. le traitement des données à des fins de santé[10] est nécessaire dans l'intérêt des personnes physiques et de la société pour les finalités suivantes :
   - La gestion des services et des systèmes de soins de santé ou de protection sociale ;
   - Le contrôle de la qualité, de l'information des gestionnaires et de la supervision générale ;
   - Assurer la continuité des soins de santé ou de la protection sociale et des soins de santé transfrontaliers.

---

[5] Voir www.corona-datenspende.de , Allemagne.

[6] Voir FAQ, Corona-datenspende.de : « *Die Nutzung der App basiert auf einer individuellen Nutzer-ID, die Ihnen persönlich zugeordnet ist – dem sogenannten Pseudonym. Nur so können Daten auch über längere Zeiträume richtig zugeordnet und interpretiert werden. Die App ist damit nicht anonym, sondern pseudonym. Dennoch hat das Robert Koch-Institut zu keiner Zeit Kenntnis Ihrer persönlichen Informationen (Anschrift oder Name).* », Allemagne.

[7] Voir Statement on the processing of personal data in the context of the COVID-19 outbreak ,EDPB

[8] Voir art 9.3, RGPD : « *Les données à caractère personnel visées au paragraphe 1 peuvent faire l'objet d'un traitement aux fins prévues au paragraphe 2, point h), si ces données sont traitées par un professionnel de la santé soumis à une obligation de secret professionnel conformément au droit de l'Union, au droit d'un État membre ou aux règles arrêtées par les organismes nationaux compétents, ou sous sa responsabilité, ou par une autre personne également soumise à une obligation de secret conformément au droit de l'Union ou au droit d'un État membre ou aux règles arrêtées par les organismes nationaux compétents* ».

[9] Considérant 52 , RGPD : « *Des dérogations à l'interdiction de traiter des catégories particulières de données à caractère personnel devraient également être autorisées lorsque le droit de l'Union ou le droit d'un État membre le prévoit, et sous réserve de garanties appropriées, de manière à protéger les données à caractère personnel et d'autres droits fondamentaux, lorsque l'intérêt public le commande, notamment […] à des fins d'alerte sanitaire, de prévention ou de contrôle de maladies transmissibles et d'autres menaces graves pour la santé. Ces dérogations sont possibles à des fins de santé, en ce compris la santé publique et la gestion des services de soins de santé, en particulier pour assurer la qualité et l'efficience des procédures de règlement des demandes de prestations et de services dans le régime d'assurance-maladie, [..] ou à des fins statistiques.* »

[10] Considérant 53 , RGPD

En outre le traitement doit s'accompagner de mesures techniques et organisationnelles appropriées[11] surtout dans le cadre de l'intérêt public sans le consentement de la personne physique dans le domaine de la santé publique.

L'art 15 de la directive E-privacy (= *traitement de données personnelles dans le cadre de communications électroniques*) stipule que « *les États membres peuvent adopter des mesures législatives visant à limiter la portée des droits et des obligations[...] lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale [...] ou d'utilisations non autorisées du système de communications électroniques* »,et ce, dans le cadre de l'utilisation de données de trafic[12] ou de localisation[13].

Par conséquent, le recours à la localisation des personnes physique afin de prévenir la prévenir la propagation de l'épidémie ou de contenir la contamination est, certes, louable mais pas à n'importe quelle condition ni de n'importe quelle manière.

La digitalisation et les données de localisations

Le recours à des applications de suivi de localisation entraine un risque significatif pour les droits et libertés fondamentales des personnes physiques. En effet, ces applications enregistrent le moindre déplacement, font un relevé des lieux fréquentés en ajoutant les dates et heures des mouvements répertoriés au travers d'un maillage de capteurs (*ex. antenne GSM, satellite*). Ce qui signifie que si l'utilisateur peut vérifier ses allées et venues, d'autres personnes disposant d'un accès à ces applicatifs peuvent aussi vérifier et collecter ses données. Tout comme ces applications peuvent avoir d'autres destinataires que l'utilisateur, notamment, l'opérateur TELECOM, le développeur et/ou le gestionnaire de l'app, l'employeur dans le cadre de la géolocalisation des véhicules et des employés ou des partenaires commerciaux (*ex. annonceurs, agence de communications*).

En ce qui concerne la géolocalisation dans le contexte du travail[14], le RGPD autorise le traitement moyennant :

- Un exercice d'analyse d'impact sur les droits et libertés fondamentales des personnes physiques (DPIA) ;
- Une recherche d'alternative moins intrusive ;
- Une information préalable des salariés concernés par ce traitement ;
- L'implémentation des mesures de sécurité techniques et organisationnelles appropriées (*ex. chiffrement des données transmises, gestion des accès, VPN, etc.*).

En ce qui concerne la digitalisation des services et le direct marketing[15], le RGPD et la E-privacy donne un cadre pour le traitement des données de localisation des individus sur base des éléments suivants :

- Protection des données dès la conception (Privacy By Design) ;
- Identification de la base légale du traitement ;
- Données anonymisées[16] plutôt que pseudonymisées .Ces dernières restent soumises aux exigences du RGPD ;
- Analyse d'impact sur les droits et libertés fondamentales des personnes physiques (DPIA) ;
- Information préalable de l'utilisateur concerné par ce traitement ;
- l'implémentation des mesures de sécurité technique et organisationnelle appropriées (*ex. chiffrement des données transmises, gestion des accès ,test, procédure de sélection des sous-traitants, etc.*).

---

[11] Considérant 54 , RGPD

[12] Voir art 6, E-privacy

[13] Voir art 10,E-privacy

[14] Voir art 88, RGPD

[15] Voir RECOMMANDATION n° 01/2020 du 17janvier 2020 relative aux traitements de données à caractère personnel à des fins de marketing direct , APD, Belgique

[16] Voir art 10 § 1 , E-privacy : « *Lorsque des données de localisation, autres que des données relatives au trafic, concernant des utilisateurs ou abonnés de réseaux publics de communications ou de services de communications électroniques accessibles au public ou des abonnés à ces réseaux ou services, peuvent être traitées, elles ne le seront qu'après avoir été* ***rendues anonymes ou moyennant le consentement des utilisateurs*** *ou des abonnés, dans la mesure et pour la durée nécessaires à la fourniture d'un service à valeur ajoutée.* »

Les 7 principes du RGPD[17]

Les applications utilisant des données de localisations sont soumises aux exigences du RGPD indépendamment du fait qu'elles traitent des données de l'utilisateur dans le cadre de communication électroniques. La directive E-privacy couvre l'utilisation du réseau de services communications électroniques accessibles au public *(=le canal ou le moyen de communication*), le RGPD porte sur le support et le contenu de la communication d'information.

1. **licéité : quelle est la base légale ?**

Le fondement juridique dépend du traitement, du rapport avec la personne concernée et du rôle de celui qui traite les données : responsable de traitement ou sous-traitant ?

- Le contrat : par l'exécution d'une convention qui lie les parties ;
- L'obligation légale : par l'application d'une disposition légales et réglementaires (ex. les circulaires de régulateurs) ;
- L'intérêt vital ;
- L'intérêt public : en fonction d'une mission d'intérêt public (*ex. loi créant un institut*) ;
- L'intérêt légitime : vérifier la balance des intérêt du responsable de traitement face aux droits et libertés fondamentales des personnes physiques (*ex. vidéo-surveillance*) ;
- Le consentement : résiduel, à l'exclusion des 5 autres (*ex. formulaire de contact d'un site internet, abonnement à une newsletter, cookies, ...*) ou en cas de traitement ultérieur non identifié préalablement dans un contrat.

2. **L'exactitude : les données sont-elles correctes ?**

Le responsable de traitement est tenu de vérifier que les données sont bien exactes, légitimes et adéquates.

3. **Minimisation des données**

Il est recommandé de n'utiliser que les données strictement nécessaires. Il est préconisé d'avoir recours à la pseudonymisation voire l'anonymisation. Dans ce dernier cas, le RGPD ne s'applique plus.

4. **Spécification des finalités**

Les données ne sont utilisées que pour les finalités pour lesquelles elles ont été collectées.

5. **La conservation : combien de temps est-ce nécessaire de garder les données ?**

Les données sont effacées ou détruites dès qu'elles ne sont plus nécessaires au traitement. Les données utilisées à des fins archivistiques ou statistiques peuvent être conservées à plus long terme moyennant leur anonymisation[18].

6. **La sécurité : sécurité des locaux et du système d'information**

Des mesures de sécurité techniques et organisationnelles appropriées doivent être mise en place :

- *Pseudonymisation et le chiffrement*: protocoles (ex. TLS, SSL, Https, IPsec), structure et architecture de base de données, réseau, etc…
- *Garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement* : politique de sécurité, charte IT ,notice d'information, VPN, gestion des accès (IAM,MDM),le transfert hors de l'Union européenne (*ex. cloud*), etc...
- *Rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique* : plan de continuité d'activité (PCA - BCP), plan de reprise d'activité (PRA - DRP),…
- *une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et*

[17] Voir art 5, RGPD
[18] Voir art 89.1, RGPD

organisationnelles pour assurer la sécurité du traitement : test fonctionnel, test utilisateur, audit interne,…

7. L'accountability

Le responsable de traitement agit en « *bon père de famille* » et prend les actions qui s'imposent de sorte qu'il puisse démontrer le respect des exigences du RGPD notamment en appliquant les principes énoncés *infra* (*ex. tenue d'un registre de traitement des activités, procédure d'alerte en cas de violations de données, gestion de l'exercice des demandes de droits des personnes concernées, etc.*)

Le développement d'application digitale

La création d'applicatif relève souvent d'idée innovante utilisant des techniques tantôt intrusives tantôt plus ouvertes**.** Le cadre de la protection des données n'a pas pour vocation de limiter la transformation digitale mais de circonvenir à tout utilisation abusive de données personnelles : ces applicatifs sont de plus en plus tournés vers l'extension de service à la personne dans sa vie quotidienne mais nécessite en retour que nous fournissions des éléments personnels de sorte à bénéficier d'une utilisation adéquate du service offert.

En tout état de cause, un applicatif exige des données (*data = ce que nous utilisons*), de la logique dans le traitement de ces données (*logique= comment nous les utilisons*) et un rendu visuel du traitement de ces données (*vue= ce vous voyez à l'écran*). Ce processus répond aux objectif suivants *(= finalités*) :

- Partager différentes informations relatives aux produits et services fournis ;
- Suivre la gestion des demandes d'information et/ou de contact ;
- Optimiser l'interface et d'assurer la sécurisation du système d'information ;
- Le traitement doit avoir une base légale (*ex. contrat avec un opérateur*) mais d'autres traitements sont basés sur votre consentement (*ex. case à cocher*) , ce qui signifie que l'on soumettra la demande future de contact ou d'autre traitement ultérieur à votre consentement préalable.

1. Privacy by design

Selon, l'art 25 du RGPD, tout service ou produit doit intégrer les principes de protection des données dès la conception : ce qui signifie que lors de la phase créative, le concepteur doit se poser une série de question avant d'entamer le développement de son projet :

- Des données personnelles sont-elles nécessaires ? si oui, lesquelles ? sont-elles toutes nécessaires ?
- Pourquoi ai-je besoin de ces données ? quelles sont les finalités ?
- Le traitement présente-t-il un risque pour les personnes physiques dont je collecte les données ?
  - Oui : j'effectue une analyse d'impact
  - Non : je prends des mesures appropriées pour garantir la sécurité
- Comment garantir la sécurité du traitement ?
- Combien de temps les données doivent-elles être conservées ?
- Où sont-elles sauvegardées ?
- Y-a-t-il utilisation d'un service cloud situé en dehors de l'union européenne ?
- Qui a accès aux données ?
- A qui sont-elles transmises ?

Chaque réponse va fournir une indication sur les exigences à respecter.

Remarque :
Les 7 principes fondamentaux[19] du privacy by design recouvrent une partie des principes RGPD :

-prévoir et de prévenir les incidents liés à l'atteinte de la vie privée avant même qu'ils ne se produisent.
-faire en sorte que les données personnelles soient protégées de manière automatique avec un paramétrage par défaut des nouvelles technologies assurant un niveau de protection maximum des données sans que l'utilisateur ait à définir de paramètres spécifiques.
-Intégrer la protection de la vie privée dans la conception des systèmes et des pratiques.
-assurer la protection de la vie privée sans nuire à la mise en œuvre d'autres fonctionnalités.
-assurer la sécurité de bout en bout, pendant toute la période de conservation des données
-chaque élément intégré aux systèmes lié à la protection des données personnelles doit rester visible et transparent en cas de vérification indépendante.
-Respecter la vie privée des utilisateurs.

La principale différence réside dans le fait qu'ils s'appliquent essentiellement au système d'information et développement d'applicatif alors que le RGPD s'applique à tout traitement de données personnelles automatisé ou non[20].

2. Analyse d'impact (DPIA)

Lors du recours à de nouvelles technologies, certains traitements peuvent engendrer un risque élevé pour les droits et libertés fondamentales des personnes physiques (*ex. transmission d'un état de santé en clair*). Dans ce cas, une analyse d'impact devra être effectuée avant d'entamer le traitement.

Les critères d'éligibilité[21] d'une analyse d'impact sont les suivants :

- **l'évaluation systématique et approfondie d'aspects personnels** concernant des personnes physiques, qui est fondée sur un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire ;
- le traitement à **grande échelle de catégories particulières de données** (art 9) ou de données à caractère personnel relatives à des condamnations pénales et à des infractions (art10) ;
- la **surveillance systématique à grande échelle d'une zone accessible au public**.

Remarque *:*
Il est important de noter le rôle du DPO dans le cadre de l'analyse d'impact : à la demande du responsable de traitement, il conseil et vérifie l'exécution de cette dernière[22] .
*Tout organisme ne doit pas désigner un délégué à la protection des données (**D**ata **P**rotection **O**fficer).*

Une liste du WP 29[23] publiée sur le site du CEPD reprend les principaux traitements à risque. Il est aussi conseillé de vérifier la liste publiée par l'autorité de contrôle nationale.

Les applicatifs collectant les données de localisations relèvent du 3éme critère.

Au Luxembourg ,la CNPD[24] a repris ce traitement dans la liste des opérations de traitement pour lesquels une AIDP est requise : «*Les opérations de traitement qui consistent en un suivi systématique de la localisation de personnes physiques* » [25]

---

[19] Voir Privacy by Design: The 7 Foundational Principles - Implementation and Mapping of Fair Information Practices , Ann Cavoukian, Ph.D. Information & Privacy Commissioner, Ontario, Canada
[20] Voir art 2.1, RGPD : « Le présent règlement 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. »
[21] Voir art 35, RGPD
[22] Voir art 35 et 39 , RGPD
[23] Voir wp248rev.01, EPDB
[24] CNPD est la **C**ommission **N**ationale de **P**rotection des **D**onnées du Grand-Duché de Luxembourg.
[25] Voir Analyse d'impact relative à la protection des données, CNPD

En Belgique, l'autorité belge de protection des données (APD - GBA) identifie les opérations suivantes s'appuyant sur des canaux de communication ou d'échanges d'informations[26] :

- *lorsqu'il est question d'un traitement à grande échelle de données générées au moyen d'appareils dotés de capteurs qui envoient des données via Internet ou via un autre moyen (IOT)[…] et que ce traitement sert à analyser ou prédire la situation économique, la santé, les préférences ou centres d'intérêt personnels, la fiabilité ou le comportement, la localisation ou les déplacements de personnes physiques ;*
- *lorsqu'il est question de traitements de données à caractère personnel à grande échelle où le comportement de personnes physiques est observé, collecté, établi ou influencé[…] ;*

En France, la CNIL a publié 2 listes , l'une pour les opérations ne nécessitant pas une analyse d'impact et l'autre concernant les opérations pour lesquelles elle est requise.

La CNIL a identifié 2 types d'opérations susceptibles[27] d'être incluses par les applicatifs de localisations développés pour endiguer la propagation du virus:

- *traitement utilisé par une agence sanitaire pour la gestion d'une crise sanitaire ou d'une alerte sanitaire ;*
- *Application mobile permettant de collecter les données de géolocalisation des utilisateurs*.

L'autorité de contrôle française est allée plus loin en développant un outil d'analyse téléchargeable (version Web – logiciel) : PIA

3. Les finalités et la base légale
   - organisme privé (*ex. société commerciale, associations, start-up , etc.*) :
     - le contrat (= *convention qui lie l'utilisateur et le propriétaire de l'applicatif , le développeur devient alors un sous-traitant*) ;
     - l'intérêt légitime ou le consentement : utilisation des données collectées grâces aux applicatifs auxquels l'utilisateur se connecte.(*ex. géolocalisation et navigation ,GPS, marketing, profilage*) ;
     - l'intérêt public : investi d'une mission par une autorité publique (*ex. guichet en ligne des autorités ou un applicatif développé par une société privée à la suite d'un appel d'offre dans le cadre d'une mission d'intérêt public*) ;
   - organisme de droit public (*ex. communes, agences gouvernementales, GIE, ministères, gouvernements*) : mission d'intérêt public si cet applicatif ressort directement de ses missions.

La base légale est déterminée par le rapport existant entre la personne concernée et le responsable de traitement.

4. La sécurité

Les applicatifs doivent impérativement être des espaces de communication sûrs et garantir la transmission de données personnelles de manière la plus sécurisée possible. Le RGPD instaure un régime de mesures de sécurité techniques et organisationnelles appropriées, c'est-à-dire, adaptées ou modulées en fonction des critères suivants :

- Les données personnelles pseudonymisées voire anonymisées, à défaut, un cadre sécurisé doit être implémenté ;
- Favoriser les techniques de chiffrement (*ex. clés, protocoles de sécurité, QR Code*) ;
- Intégrer une gestion des accès structurée et hiérarchisées (*ex. IAM,MDM*) ;
- Tester les scénarios de fonctions applicatives et d'utilisations diverses, d'incident de sécurité ;
- Prévoir un système de récupération des données en cas d'incident ;
- Informer l'utilisateur sur les fonctionnalités et les limites d'utilisations.

En ce qui concerne les statistiques, il faut distinguer les statistiques de métadonnées (*ex. logs, cookies*) qui vont permettre l'optimisation du service, des fonctionnalités en analysant le comportement de l'utilisateur et les statistiques de données personnelles afin d'établir des profils d'utilisateur. Le RGPD préconise le recours à la pseudonymisation

[26] Voir Adoption de la liste des catégories de traitement devant faire l'objet d'une analyse d'impact relative à la protection des données conformément à l'article 35.4 du Règlement Général sur la Protection des données (CO-A-2018-001) , APD, Belgique

[27] Voir Liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise , CNIL, France

afin de prévenir l'atteinte aux droits et libertés fondamentales des personnes physiques.

En ce qui concerne les données de santé , il faut impérativement établir des protocoles de sécurité assurant une transmission des données aux personnes concernées et sélectionner rigoureusement les sous-traitants[28]. Un audit de ces fournisseurs est d'ailleurs fortement recommandé.

5. Information préalable au traitement

Dans le cas d'applicatif utilisant des données de localisations pour endiguer la contamination, il y a croisement de données qui donne lieu à un profilage des personnes physiques:

- Des métadonnées liées à l'appareil et aux comportement de l'utilisateur : Où suis-je situé ? (= *donnée d'identification et de localisation*)
- Des données liées à l'état de santé : suis-je positif ? suis-je infecté ? *(=donnée de catégorie spéciale*)

Ces traitements requièrent des précautions d'usage quelle que soit la qualité du responsable de traitement (autorité publique ou organisme privé) :

- une analyse d'impact préalable
- une sécurité accrue dans la transmission des données de sorte que les données personnelles soient anonymisées avant qu'elles ne tombent entre les « doigts » de personne mal intentionnée (*ex. violation de données et cybersécurité*)
- une information préalable de l'utilisateur

Pour l'organisme public :

- l'information spécifique relative aux traitements aux fins de médecine préventive et de protection contre les menaces transfrontalières graves pesant sur la santé (art 9.2.h et i)

Pour l'organisme privé :

- le recueil du consentement de l'utilisateur (art 9.2.a)

6. L'exercice des droits des personnes concernées

Cette obligation découle de la précédente : lorsque le responsable de traitement informe les personnes concernées, il est tenu d'indiquer comment l'exercice des droits est possible[29]. Dans le cadre d'application, il est possible de permettre l'exercice de ces droits via un formulaire en ligne.

Les avantages :

- Il est directement et facilement utilisable par l'utilisateur ;
- Il peut être lié à la gestion du profil de l'utilisateur par lui-même (*ex. gestion de compte et paramétrage de l'application*) ;
- Il peut être intégré aux fonctionnalités de l'applicatif (*ex. paramétrage des notifications, newsletters*) ;
- Il garantit que la personne concernée est bien l'utilisateur de l'application : ce dernier étant connecté, la vérification de l'identité n'est pas nécessaire dans ce cas[30].

Les inconvénients

- L'utilisateur n'a pas toujours la connaissance pour distinguer les droits et leur conséquences (*ex limiter le traitement, s'opposer ou retirer son consentement*) ;
- Le formulaire est trop détaillé ou trop vague ou il implique une gestion avancée du compte utilisateur.

[28] Voir art 28.3 h, RGPD

[29] Voir art 13.2 b, RGPD

[30] Les règles d'authentifications (*ex. double authentification*) forment un 1ier test pour prévenir l'usurpation de compte et/ou d'identité.

Article : RGPD – Le virus et l'application digitale

Conclusion

Les défis de l'humanité sont caractéristiques de la période historique pendant laquelle ils se déroulent et les moyens de lutter contre la maladie et les épidémies reflètent les époques : on identifie les malades et on les isole du reste du groupe dans des conditions parfois difficiles. A l'ère de la transformation digitale, on utilise les réseaux de communication pour identifier, vérifier et décider qui doit être isolé du groupe. L'individu, personne physique, devient une donnée que l'on traite selon des protocoles définis par des autorités et ce, souvent, au détriment de la liberté individuelle. La protection des données à caractère personnel prévient ,dans une certaine mesure, cette ingérence et rétablit l'équilibre entre mesures imposées d'autorité et droits et libertés fondamentales.

A nous de préserver notre espace individuel tout en adhérant au principe de santé publique et bien-être pour tous.

Prenez soin de vous et de vos proches.

Cathy Vranckx
Consultante en protection des données.

#Resteràlamaison #Stay@home