Communiqué de Presse

La CNDP à la disposition du gouvernement pour renforcer, en termes de respect de la vie privée, ses politiques proactives.

Rabat, le 16 avril 2020.

La CNDP a pris connaissance, par voie de presse, de la volonté du gouvernement de mettre en place une application de « contact tracing ».

Cette annonce a immédiatement généré, une interrogation, et voire, une inquiétude citoyenne autour des risques de déploiement d'un Etat de surveillance dans le cas où les usages permis par cette application n'étaient pas respectueux des droits humains et encadrés juridiquement.

La loi 09-08, en alignement avec l'article 24 de la Constitution du Royaume, confère à la CNDP la mission publique de contrôle de la protection des données à caractère personnel et de la vie privée, en particulier au sein de l'écosystème numérique.

Les concepts de minimalité et de proportionnalité font partie des outils d'appréciation qui permettent d'évaluer, dans le cadre d'une analyse des risques élargie, le pour et le contre de chaque usage au regard du respect de la vie privée, mais aussi au regard des autres droits fondamentaux.

La gravité de la situation sanitaire et les évolutions observées au travers des courbes de propagation des contaminations, mais aussi celles à gérer lors des phases de déconfinement à venir, constituent un risque majeur.

Ainsi, pour maîtriser la propagation de la pandémie, en particulier lors de la phase de déconfinement à venir, nous ne pouvons nous permettre, pour l'intérêt collectif, de nous tromper de combat.

Il est louable que le gouvernement anticipe, et la CNDP salue le courage politique et opérationnel avec lequel le ministère de la santé et le ministère de l'intérieur adoptent cette démarche proactive.

Cependant, la CNDP insiste sur la nécessité de conforter la confiance, en particulier la confiance numérique : Si celle-ci n'est pas assurée, le nécessaire large usage de l'application s'en trouvera affecté et les résultats escomptés altérés.

Il est recommandé que l'usage de ce type d'application soit déployé sur la base d'une confiance volontariste et non sur la base d'une obligation difficile à mettre en œuvre.

Pour assurer cette condition sine qua non de confiance concernant la collecte et l'utilisation des données à caractère personnel, la CNDP recommande fortement au gouvernement de :

- Veiller à garantir la complémentarité annoncée comme nécessaire entre le **pistage** et l'usage de cette application, d'une part, et la politique de **dépistage** et de tests au COVID19, d'autre part. Ces deux dispositions vont de pair. L'insuffisance du dépistage peut remettre en cause l'intérêt du pistage.
- Justifier que cette complémentarité et les algorithmes utilisés répondent effectivement à la finalité du contrôle de la propagation de la pandémie.

- Veiller à définir, de façon explicite, la finalité stratégique et les moyens opérationnels et techniques pour l'atteindre. La finalité stratégique est le contrôle de la propagation de la pandémie. Les moyens opérationnels et techniques pour l'atteindre doivent distinguer les moyens de type « tracing » induits par des technologies comme le bluetooth et les moyens de type « tracking » induits par des technologies comme la géolocalisation et le GPS. Les moyens utilisés doivent être adéquats avec la finalité stratégique.
- Veiller à informer, en application du principe de transparence, l'utilisateur ciblé de la finalité affichée et des moyens utilisés pour l'atteindre.
- Veiller à ce que seules les autorités dûment habilitées (sanitaires, mais aussi le personnel d'autorité régulièrement affecté afin de faire respecter les décisions sanitaires), soient en mesure d'accéder, chaque agent selon ses missions, aux seules données à caractère personnel, jugées nécessaires à l'exécution de ses missions propres en conformité avec la finalité affichée.
- Veiller à ne pas réutiliser les données à caractère personnel autrement que pour la finalité affichée.
- Veiller à détruire les données collectées et générées à la sortie de l'état d'urgence sanitaire, sauf celles pouvant alimenter, de façon anonymisée et réglementaire, la recherche scientifique.
- Prendre en considération que l'administration, vu la sensibilité du sujet, ne peut recourir à l'acquisition de boîte noire (black box). Elle doit être en maîtrise complète des codes développés et des architectures mises en œuvre.
- Veiller à partager, voire rendre publics, le code développé, les architectures et les technologies utilisées en autorisant leur audit citoyen, ce qui permet aussi de respecter le principe de la publication proactive mais aussi de la procédure d'urgence prévue par la loi n°31-13 relative au Droit d'Accès à l'Information. Cet audit peut être également sollicité, par tout autre acteur, selon les mécanismes constitutionnels existants.

La CNDP se tient à la disposition des autorités gouvernementales pour les accompagner à conforter le cadre de confiance numérique pouvant contribuer à gérer les deux priorités du moment : la gestion du risque sanitaire et le maintien de l'activité économique.

La CNDP se tient également à la disposition des citoyens pour répondre à leurs interrogations et suivre leurs craintes et inquiétudes au sujet du non-respect de leur vie privée et de leurs données à caractère personnel.

La CNDP prend bonne note des efforts menés, depuis sa création, par la CDAI (Commission du Droit d'Accès à l'Information) pour la mise en œuvre des dispositions de la loi 31-13 et qui contribuent à conforter la confiance numérique.

La CNDP, en vue de réaliser un rapport sur le respect de la protection des données à caractère personnel pendant la période d'urgence sanitaire, sollicitera les administrations concernées pour recueillir toutes les informations utiles à cet effet.

La CNDP est confiante sur le fait que, grâce à l'interaction constructive des différents acteurs, notre pays est en train d'utiliser son intelligence collective pour jeter les bases d'un nouveau départ.