Recréer la confiance entre citoyens et représentants? C'est toujours possible

La démocratie directe a l'énorme avantage de connecter les citoyens à la décision publique et de maintenir ainsi la confiance entre citoyens et dirigeants.

Frédéric Mauro

Chercheur associé à l'Iris et avocat au barreau de Bruxelles

La pandémie actuelle n'a fait qu'ouvrir béante une «fracture sociale» qui existait depuis longtemps, et pas seulement en France. Car le constat vaut dans toutes les démocraties représentatives: Trump, Brexit, gilets jaunes, les symptômes sont différents mais la cause est la même: la défiance des citoyens envers leurs institutions, leurs dirigeants, envers les médias et même envers les experts devenus soudainement inutiles dans une société où la vérité importe de moins en moins.

Trump a perdu les élections, mais des millions d'Américains croient que ce n'est pas vrai. Le vaccin protège, mais beaucoup n'en veulent pas. Or sans quelques vérités partagées, il ne peut y avoir de société harmonieuse.

Les vrais héros de la liberté

Dernière manifestation de ce mal profond et contagieux, le rejet par quelques centaines de milliers de Français du pass sanitaire. Or pour préserver leur «liberté», les manifestants foulent aux pieds celle des autres.

Quand la liberté des uns ne s'arrête plus où commence celle des autres, alors commence le règne de l'anarchie et du chacun pour soi. Autant supprimer le permis de conduire.

Non, les vrais héros de la liberté ne sont ni à Paris, ni à Marseille, mais à Hong-Kong, à Moscou et à Minsk. Il serait temps que les enfants de Descartes retrouvent la raison et cessent d'affubler tout représentant du nom de dictateur.

Pour autant, ne jetons pas l'anathème facile du «complotisme» et tâchons de comprendre comment nous sommes passés d'une société où les citoyens avaient confiance dans la parole publique, depuis l'école jusqu'à l'université, à une société où la défiance est devenue la règle et la révolte son expression.

Manifester, crier, casser

L'une des explications les plus communément admises est que les dirigeants nationaux ont vu leur pouvoir s'évaporer vers d'autres cadres: le «Monde», «l'Europe», les «réseaux sociaux». Le problème est qu'il ne suffit pas de sortir de l'Union européenne pour retrouver le contrôle et que la «démondialisation» n'est qu'une formule creuse. Voter Giscard ou Mitterrand, ce n'était pas la même chose. Mais entre Sarkozy et Hollande quelle différence? Si tout ça ne sert à rien alors pourquoi voter? Mieux vaut manifester, crier et casser.

Nous sommes entrés dans un cercle vicieux, car la confiance est à la fois une condition et un résultat du bon fonctionnement d'une société. Sans confiance les dirigeants ne peuvent pas diriger et voient leurs décisions contestées. Mais s'ils ne peuvent pas diriger, alors la confiance ne peut s'instaurer et sans confiance entre ses membres aucune société ne peut prospérer.

La question est donc: comment recréer la confiance? Des expériences de «démocratie participative» ont bien été tentées, pour remettre les citoyens au centre du jeu démocratique, en France avec la convention citoyenne, comme en Belgique avec les «commissions délibératives», mais les résultats peinent à convaincre.

> Quand la liberté des uns ne s'arrête plus où commence celle des autres, alors commence le règne de l'anarchie et du chacun pour soi. Autant supprimer le permis de conduire.

L'exemple suisse

Or, il y a un moyen de faire participer les citoyens aux décisions politiques, aussi vieux que la démocratie elle-même et pratiqué régulièrement par nos amis helvètes: la démocratie directe.

Les «votations populaires» ne produisent pas nécessairement des décisions meilleures ou plus rationnelles que celles des représentants de la nation. Mais la démocratie directe a l'énorme avantage de connecter les citoyens à la décision publique et ainsi de maintenir la confiance entre citoyens et dirigeants. C'est peut-être le remède dont nous avons tant besoin.

Si le pass sanitaire est à ce point contesté en France que l'on organise donc un referendum. Le peuple souverain décidera. Pour de bon cette fois.

Revue de presse

A quand un débat sérieux sur les passeports vaccinaux?

THE GUARDIAN

Nous devons avoir un débat national à propos du passeport vaccinal. Le problème posé par l'approche catastrophique du gouvernement, qui consiste à donner la priorité à l'économie dans la gestion de la pandémie, n'est en effet que trop évident.

L'introduction d'un passeport domestique sera coûteuse, de nature à diviser, contre-productive et dangereuse pour notre mode de vie.

Nombreux sont ceux au sein du gouvernement qui ont déjà fait volte-face sur la question de savoir s'il fallait exiger une preuve du statut vaccinal avant d'accéder à une série d'activités quotidiennes. Des messages tout aussi contradictoires ont été envoyés quant à savoir si une telle mesure devait être laissée à l'appréciation des entreprises.

Cette instabilité constante est, en fait, moins le signe d'un manque de compétence que celui d'un chaos malveillant et étudié visant à renvoyer la balle pour toute nouvelle victime de la pandémie. Cette approche, l'immunité collective 2.0, laisse en effet le virus proliférer et crée un territoire fertile pour les variantes résistantes au vaccin.

À cet égard, le passeport vaccinal est une mesure illibérale et discriminatoire; un moyen de forcer les jeunes à se faire vacciner plutôt que de prévenir efficacement la transmission.

La vaccination obligatoire est contre-productive dans les pays de tradition libérale et libertaire. Elle est aussi contraire à l'éthique étant donné la nouveauté de ces vaccins et le manque d'éducation du public.

Les passeports domestiques, quels qu'ils soient, mènent inévitablement à la discrimination, à la corruption et à l'oppression. Et étant donné que ce nouveau type de carte d'identité obligatoire concerne explicitement la santé, ils franchissent une nouvelle limite en matière de vie privée et de liberté.

Les passeports domestiques covid font en réalité partie d'une stratégie de poudre aux yeux d'un gouvernement qui aimerait croire que la «responsabilité personnelle» peut se substituer à une politique de santé publique saine et éthique face à une pandémie qui a déjà coûté au Royaume-Uni près du double des pertes civiles encourues durant la Seconde Guerre mondiale.

L'heure n'est plus aux jeux politiques. Il est grand temps d'avoir un débat honnête sur la manière dont nous voulons nous protéger mutuellement.

L'expert

Steven De Ruyver *Security Lead de Cisco Belux*

Ransomware: payer ou ne pas payer?

Si vous disposez de sauvegardes sûres et de politiques de cybersécurité strictes, ne payez pas les rançons. 80% des entreprises qui ont été piratées ont de nouveau été attaquées... par les mêmes hackers dans la moitié des cas.

En un an, les demandes en matière de services de cybersécurité ont triplé. Alors que les grandes entreprises ont généralement les ressources pour se protéger, les PME apparaissent comme des cibles parfaites pour les cybercriminels. Récemment, la société belge ITxx a ainsi payé 350.000 USD de rançon pour éviter une fuite de ses données. Elle a cédé à ses ravisseurs, mais a eu le courage de signaler publiquement l'attaque. De nombreuses autres sociétés préfèrent quant à elles garder leurs mésaventures sous silence malgré une obligation de rapporter les attaques.

Comme ITxx, la plupart des organisations piratées ont eu affaire à un ransomware. Les hackers infiltrent les réseaux informatiques de leurs cibles et exigent une rançon pour ne pas divulguer les fichiers importants. Un vrai dilemme: faut-il payer ou non?

La solution la plus juste est de refuser. Accepter est toutefois plus simple. Cette dernière option ne devrait toutefois être utilisée uniquement que si l'on n'a pas d'autre choix. La question devient en effet extrêmement épineuse lorsque la survie d'une entreprise en dépend. Dans ce cas, il n'y a plus de «bon» ou de «mauvais» choix moral.

Il y a quelques années, la ville d'Atlanta avait décliné le paiement d'une rançon de 50.000 $. En revanche, elle a investi près de 17 millions de dollars pour restaurer et sécuriser ses serveurs.

L'an dernier, les paiements de rançons ont augmenté de 170%. Les sociétés américaines JBS et Colonial Pipeline ont récemment décidé de payer leurs hackers en bitcoins. Et pour cause, aux États-Unis, les dépenses pour des cyberattaques sont déductibles des impôts.

Les polices d'assurance en matière de cybersécurité n'incitent guère également à adopter des approches proactives. Certains assureurs belges ont d'ailleurs purement et simplement supprimé leurs polices en matière de cybersécurité.

En payant la rançon, vous financez les personnes qui tentent de vous extorquer. Vous faites confiance aux hackers sans garantie qu'ils ne divulgueront pas vos données après coup. Quand nous étions plus jeunes, si une brute prenait notre argent de poche, nous pouvions être sûrs qu'elle reviendra nous vandaliser.

80% des entreprises qui ont été piratées ont de nouveau été attaquées, et ce par les mêmes responsables dans la moitié des cas. Si vous avez des sauvegardes sûres et des politiques de cybersécurité strictes, ne payez pas les rançons. Il faudra en revanche l'envisager si votre sécurité n'est pas optimale. Dans ce cas, prévoyez d'investir immédiatement dans une sécurité numérique complète.

Multipliez les obstacles numériques

Plus il sera difficile d'infiltrer vos réseaux informatiques, moins les cybercriminels tenteront leur chance. Investissez dans la sécurité, segmentez vos réseaux et créez de meilleurs mots de passe. Encore aujourd'hui, beaucoup trop de mots de passe évidents sont utilisés. Heureusement, les authentifications multifacteurs deviennent de plus en plus courantes.

En matière de cybersécurité, l'humain est le maillon faible. Les écoles et les universités ont un rôle à jouer pour sensibiliser à la cybersécurité. Malheureusement, cette étape est au point mort pour le moment. Pendant ce temps, les cybercriminels s'organisent de plus en plus. Vous pouvez aujourd'hui louer un logiciel en tant que service afin de pirater quelqu'un.

> En payant la rançon, vous financez les personnes qui tentent de vous extorquer. Vous faites confiance aux hackers sans garantie qu'ils ne divulgueront pas vos données après coup.

Pour autant, les attaques à grande échelle diminuent (car elles sont facilement détectables), mais elles sont en revanche de plus en plus ciblées. Des formations et des campagnes de sensibilisation aideraient certainement les utilisateurs à rester davantage attentifs aux menaces.

Coopération internationale renforcée

Le problème des ransomwares est désormais mondial. Tant mieux, cela favorise la coopération entre les pays. Le ministère américain de la Justice, Europol et des leaders mondiaux de l'informatique ont d'ailleurs créé à cet égard la «Ransomware Task Force»; un rassemblement qui a pour but d'unir les forces dans la lutte contre les cyberattaques.

En ce qui concerne l'e-banking, votre banque demeure responsable de la sécurité de vos données. Dans les autres secteurs du numérique, la cybersécurité est une responsabilité partagée. Une organisation comme la «Ransomware Task Force» sera-t-elle suffisante? Il est encore trop tôt pour le dire. Les cybercriminels innovent en effet permanence pour parvenir à leurs fins. Nous devons faire de même.