Intervention de Gianni Buquicchio à la 15e Conférence européenne des administrations électorales sur la sécurité dans les élections

19-20 avril 2018, Oslo, Norvège

Madame la ministre,

Monsieur le Secrétaire Général,

Mesdames et Messieurs membres des corps diplomatiques et représentants des autorités de la Norvège,

Mesdames et Messieurs les présidents d'administrations électorales,

Mesdames et Messieurs,

Chers amis,

C'est un honneur pour moi d'inaugurer aux côtés d'éminentes personnalités la 15e Conférence européenne des administrations électorales, consacrée à la sécurité dans les élections.

15 conférences européennes des administrations électorales signifie, Mesdames et Messieurs, pas moins de 15 années de rencontres autour de thèmes liés aux élections.

Ces 15 éditions ont permis à un nombre grandissant d'administrations en charge de la gestion des élections, ainsi qu'à d'autres spécialistes électoraux, de se retrouver afin d'échanger, promouvoir et diffuser leur savoir-faire et leur expertise en matière électorale, et de rappeler les normes et standards internationaux, qui doivent être reflétés tant dans la législation que dans la pratique nationales.

Dès la deuxième édition des conférences, la Commission de Venise a co-organisé cet événement annuel qui a gagné en importance avec le temps.

Progressivement, la participation a augmenté, en nombre de participants comme en nombre d'Etats représentés. Nous comptons pour cette édition 160 participants, provenant de plus de 40 pays d'Europe, d'Afrique, d'Asie centrale et d'Amérique Latine.

Des sujets aussi variés que la lutte contre la fraude électorale, le vote à distance ou encore la lutte contre l'abus de ressources administratives ont été débattus. Ce qui doit avant tout être retenu, c'est que nous avons, que vous avez, Mesdames et Messieurs, toujours traité des thèmes actuels et essentiels pour l'administration des élections. Cela est encore plus vrai aujourd'hui : le thème de ce jour est au centre de l'actualité.

Venons-en donc au sujet de notre conférence. Je commencerai par une citation :

C'est la grande sagesse du peuple, voyez-vous. Les gens ne se dérangent que pour les élections qui ont un sens (Globalia (2005) de Jean-Christophe Rufin).

Pour que les élections aient un sens, elles doivent assurer la liberté de vote, et ceci sous ses deux aspects - de libre formation et de libre expression de la volonté de l'électeur, comme le rappelle le Code de bonne conduite en matière électorale de la Commission de Venise. Ce but est réalisé, en premier lieu, à travers l'organisation des élections.

La libre formation comme la libre expression de la volonté de l'électeur impliquent que la sécurité soit garantie tout au long du processus électoral, avant, pendant et après le jour de l'élection. Il incombe aux administrations électorales d'anticiper les éventuels problèmes de sécurité et de mettre en place des mécanismes adaptés pour les résoudre, avec bien entendu la coopération des institutions de l'Etat.

Qu’est-ce que la sécurité électorale ?

Il s’agit en premier lieu de d’assurer la sécurité au sens classique : sécurité des citoyens et des candidats, des bâtiments et des installations dédiés aux élections, face à des personnes malveillantes qui pourraient vouloir troubler directement le processus électoral.

Il s’agit également de votre sécurité, administrations électorales et institutions publiques, de votre sécurité personnelle et de celle des installations dont vous avez la responsabilité !

Evidemment, ces questions de sécurité sont d’autant plus importantes lorsque des élections sont organisées à l’issue d’un conflit ou dans un contexte d’état d’urgence.

A l’époque actuelle, la sécurité électorale recouvre également, naturellement, la CYBERsécurité.

Qu’entend-on par-là ?

Il s’agit à la fois de la sécurité des installations informatiques des partis politiques et des candidats et de celle des serveurs publics stockant des informations stratégiques et des données personnelles.

Aujourd’hui, les technologies de l’information et de la communication sont constamment présentes dans les activités humaines, et cela vaut aussi pour les différentes étapes de tout processus électoral.

Les technologies de l'information et de la communication sont utilisées, par exemple, lors de l'enregistrement des électeurs, du dépouillement des votes, ou encore du transfert des résultats. Elles le sont évidemment aussi lorsqu'un système de vote électronique est appliqué.

La technologie informatique a, certes, le potentiel de rendre les processus électoraux plus efficaces, plus rapides et plus sûrs. Mais elle peut être aussi une faiblesse.

Plusieurs Etats ont, par exemple, fait dernièrement l'objet de tentatives plus ou moins avancées de cyber-attaques lors de la tenue d'élections.

Cela conduit, dans le débat public, à des réticences envers l'innovation technique, alors que, en sens inverse, des appels à plus d'informatisation pour éviter les interférences dans un processus manuel retentissent aussi.

En même temps, les technologies de l'information et de la communication sont aussi présentes dans la communication quotidienne entre les citoyens d'une part et les candidats, les partis politiques et les autorités d'autre part, et entre citoyens, notamment via les réseaux sociaux.

La cybersécurité n'est donc pas seulement l'affaire des pays qui votent par voie électronique, loin de là, mais elle est l'affaire de tous les Etats !

Les partis politiques et les candidats recourent constamment aux technologies de l'information et de la communication pour communiquer et faire campagne, y compris lorsqu'il s'agit de partager des informations sensibles.

Ainsi, les piratages et cyber-attaques touchent tout à la fois les autorités, les partis, les candidats, et même les citoyens, via les réseaux sociaux !

Et, même lorsque la sécurité est en fait assurée, si des rumeurs circulent sur la vulnérabilité des systèmes d'organisation des élections, le risque est grand d'un impact négatif sur la confiance des citoyens vis-à-vis des élections et, par conséquent, des autorités.

Nous avons tous bien compris que l'enjeu est majeur. L'enjeu n'est pas seulement technique, il s'agit, beaucoup plus largement, de pérenniser la confiance dans les élections et dans les institutions.

Comme je le disais précédemment, il s'agit d'abord d'éviter autant que possible les risques d'attaques sur les élections, sur les autorités qui les organisent et sur les citoyens eux-mêmes.

Cet aspect classique de la sécurité peut être garanti, selon les circonstances, plus ou moins facilement et largement.

Il s'agit ensuite d'éviter les manipulations informatiques, et là nous n'avons évidemment pas (encore) suffisamment de recul ; il s'agit donc d'être vigilent, imaginatif et créatif.

Nous ne sommes toutefois pas devant une page blanche : le but de notre conférence d'aujourd'hui et de demain est justement de partager les expériences déjà rencontrées avec de telles manipulations et surtout les solutions qui ont été trouvées.

Dans le domaine de la cybersécurité, outre les attaques contre les systèmes informatiques eux-mêmes, il faut contrer une menace moins directe : les rumeurs et fausses informations – les fake news - qui circulent abondamment sur les réseaux sociaux et plus encore pendant une campagne électorale, de même que les fuites d'informations sensibles.

Comment lutter contre un tel phénomène tout en assurant le plus haut niveau de protection de la liberté d'expression ?

Comment assurer une campagne électorale équilibrée, qui garantisse autant que possible une égalité des chances devant le scrutin ?

Comment pérenniser, renforcer ou restaurer le sens critique de l'électeur face à la masse d'informations qu'il ou elle suit sur les réseaux sociaux ou sur les fils d'actualité ?

Mission impossible ? Autant d'éléments qui constituent un défi majeur pour la tenue d'élections démocratiques et qu'il vous reviendra de débattre, en ouvrant des pistes de réflexion, en présentant des bonnes pratiques, et, tant que faire se peut, des solutions.

Mesdames et Messieurs,

Les évènements récents concernant la protection des données des utilisateurs des réseaux sociaux, l'affaire « Cambridge Analytica », nous rappellent une évidence : il n'incombe pas seulement aux autorités étatiques d'assurer la cybersecurité électorale mais aussi aux fournisseurs d'internet.

Les entreprises privées présentent à plusieurs égards, par leurs activités, un risque d'ingérence dans les droits de l'homme.

Le Comité des Ministres du Conseil de l'Europe l'a récemment reconnu, en rappelant dans sa Recommandation no. Rec CM (2016)3 que les entreprises « en tant qu'organes spécialisés de la société remplissant des fonctions spécifiques, doivent se conformer à toutes les lois applicables et de respecter les droits de l'homme ».

Il en va de même, et à plus fort raison, pour les intermédiaires d'internet, comme le Comité des Ministres a rappelé très récemment, en adoptant en mars 2018 une Recommandations sur le rôle et les responsabilités des intermédiaires d'internet. La recommandation contient aussi des *Lignes directrices à l'attention des États sur les actions à prendre à l'égard des intermédiaires d'internet compte tenu de leurs rôles et de leurs responsabilités.*

Le Comité des Ministres a ainsi recommandé aux Etats de mettre en œuvre ces lignes directrices lors de l'élaboration et de l'application de cadres législatifs concernant les intermédiaires d'internet, conformément à leurs obligations pertinentes découlant de la Convention européenne des droits de l'homme, et d'autres Conventions du Conseil de l'Europe, et notamment la Convention sur la cybercriminalité – dont on entendra amplement parler pendant notre conférence. La législation devrait ainsi créer un environnement en ligne sûr, propice aux

communications privées et au débat public, et devrait être conforme aux normes internationales pertinentes. La recommandation insiste encore sur la transparence et la protection de la vie privée et des données à caractère personnel.

Le Comité des Ministres a également recommandé aux autorités nationales de dialoguer régulièrement, de manière inclusive et transparente, avec tous les acteurs concernés, y compris du secteur privé, des « médias de service public », de la société civile, des établissements scolaires et des milieux universitaires, en vue de partager et d'examiner des informations, et de promouvoir l'utilisation responsable des dernières évolutions technologiques liées aux intermédiaires d'internet qui ont des répercussions sur l'exercice et la jouissance des droits de l'homme, ainsi que leurs aspects juridiques et politiques.

Mesdames et messieurs, cette conférence nous offre une excellente opportunité pour un tel dialogue.

Parmi nos orateurs, nous avons des experts, des membres des EMB, des membres de la société civile, et nous pouvons également compter sur (deux) un acteur(s) majeur(s) d'internet: (les entreprises Google et) Facebook. Je tiens à les remercier de leur participation à cette conférence, nous permettant ainsi de bénéficier de la grande expérience de (deux) grands de l'Internet en plus de celle des praticiens de l'organisation des élections.

En particulier, la conférence d'aujourd'hui devait aborder les possibilités d'interaction entre les intermédiaires d'Internet et les EMB lors de la préparation et du déroulement des scrutins, ces interactions visant à garantir que le scrutin soit l'authentique expression de la liberté de formation et d'expression de la volonté des électeurs. Cela participe de la plus-value de la conférence, car ce thème n'a pas été examiné à ce jour de manière exhaustive.

Mesdames et messieurs, vous le constatez, cette conférence s’annonce riche en débats sur la sécurité dans les élections, notion protéiforme, complexe que nous nous devons de garantir à nos citoyens, nous tous acteurs des processus électoraux.

Excellente conférence à tous !