CONFERENCE OF INGOs
OF THE COUNCIL OF EUROPE

CONFERENCE DES OING DU
CONSEIL DE L'EUROPE

La société d'information – quelles avancées et quelles menaces pour les autorités publiques et les ONG ?

Rapport du débat thématique de la Conférence des OING du Conseil de l'Europe

27 Janvier 2017, Salle 1, Palais de l'Europe

Modération : Anna RURKA – Présidente de la Conférence des OING du Conseil de l'Europe

Ouverture

Anna Rurka, Présidente de la Conférence des OING, accueille :

- la Présidente du Groupe de rapporteurs sur la Démocratie (GR-DEM) du Comité des Ministres, l'Ambassadeur JUREVIČIENĖ pour l'ouverture commune du débat ;
- les délégués des Représentations Permanentes de France, Islande, République tchèque, Danemark, Finlande, Serbie et Suède ;
- La Présidente du CDDH, Brigitte KONZ
- Les experts invités Sébastien FANTI, Avocat au Barreau valaisan, élu au poste de Préposé à la protection des données et à la transparence du canton du Valais en Suisse et Jedrzej NIKLAS, Fondation PANOPTYKON (Pologne). Alexander SEGER, Chef de division de la Cybercriminalité et Silvia GRUNDMANN, Cheffe de la Division médias et internet - Direction de la société d'information et de l'action contre la criminalité, Conseil de l'Europe
- Le(s) Représentant(s) du Secrétariat.

Elle souligne l'importance du sujet du débat, en précisant qu'il s'agit non seulement de réfléchir à l'impact général du « numérique » sur les droits de l'Homme, l'éducation et la démocratie, mais surtout de mettre en débat l'accessibilité du progrès technologique, de voir comment chaque citoyen peut être protégé et se protéger contre les menaces qui peuvent facilement compromettre son droit à la vie privée. Elle donne ensuite la parole à l'Ambassadeur **JUREVIČIENĖ,** Présidente du Groupe de Rapporteurs sur la Démocratie (GR-DEM) du Comité des Ministres, en soulignant les bons contacts développés entre le Comité des Ministres et la Conférence des OING. L'Ambassadeur confirme l'importance des échanges réguliers entre le GR-DEM avec la Conférence des OING pour tisser des liens et rappelle que le sujet du débat est au cœur des préoccupations actuelles, en mentionnant la conférence sur la liberté d'expression en ligne qui se tiendra en avril 2017 à Chypre, sous la présidence chypriote du Comité des Ministres. Elle pense que les instruments développés dans le cadre de la stratégie sur la gouvernance internet devraient permettre d'appliquer les mêmes droits « online » que hors ligne; Elle a rappelé que les mesures de répression peuvent avoir un effet glaçant, et qu'il faut faire

attention aux sur- et sous- régulations. Il faut s'appliquer à bien mettre en œuvre les recommandations existantes, qui sont des instruments de défense importants pour la démocratie, à savoir :

- Déclaration du Comité des Ministres relative à la protection du journalisme et à la sécurité des journalistes et des autres acteurs des médias, adoptée le 30 avril 2014 ;
- Résolution de l'APCE 2035 (2015) sur la protection de la sécurité des journalistes et de la liberté des médias en Europe, Résolution de l'APCE 2141 (2017) Attaques contre les journalistes et la liberté des médias en Europe ;
- Résolution 2060 (2015) et Recommandation 2073 (2015) de l'APCE portant sur la protection des donneurs d'alerte ;
- la Convention du Conseil de l'Europe sur l'accès aux documents publics, signée le 18 juin 2009 qui ne nécessite plus qu'une ratification supplémentaire pour entrer en vigueur ;
- Art. 10 de la Convention européenne de sauvegarde des droits de l'homme et libertés fondamentales, portant sur l'ingérence illégale ;

Elle a conclu en insistant sur l'importance de renforcer nos démocraties en ligne.

Normes et outils élaborés par le Conseil de l'Europe : Stratégie pour la gouvernance de l'internet (2016-2019) et Guide des droits de l'homme pour les utilisateurs d'internet

Silvia GRUNDMANN, Cheffe de la Division médias et internet - Direction de la société d'information et de l'action contre la criminalité, DG I, a remercié à son tour les Ambassadeurs de vouloir échanger avec la société civile. Elle a expliqué que le Comité Directeur sur les Médias et Sociétés d'Information (CDMSI) travaille sur des e-standards qui seront soumis pour approbation au Comité des Ministres. En cas d'adoption, les Etats membres seront tenus de respecter les recommandations, mais auront également besoin de soutien pour parvenir à mettre en œuvre toutes ces normes. Ils ont à leur disposition deux sources principales :

- La stratégie concernant la gouvernance internet 2016-2019 « Démocratie, droits de l'homme et l'Etat de droit dans le monde numérique »

- Le Guide des droits de l'homme pour les utilisateurs d'internet (existant en anglais, français, albanais, arabe, bulgare, néerlandais, allemand, grec, italien, portugais, russe, serbe, espagnol, turc, ukrainien), essentiel pour la société civile qui traite des droits et des devoirs des citoyens usagers et qui permet aux gouvernements de rendre compte de leur politique. Appuyé sur la jurisprudence de la Cour européenne des droits de l'homme, il contient trois parties:
    - des recommandations classiques aux Etats membres ;
    - un guide à l'attention des citoyens ;
    - un rapport explicatif, genèse (« pourquoi et comment »).

Le CDMSI s'efforce de soutenir la mise en œuvre des normes du Conseil de l'Europe :

- Il rédige un rapport annuel pour le Secrétaire Général du Conseil de l'Europe, qui est très actif dans le domaine de l'information et soulève régulièrement les questions auprès des Etats membres. Les défis restent énormes ;
- Il étudie la situation dans les 47 Etats membres (accessibles online par pays), et analyse les filtrages, blocages, éliminations de documents.

Il serait souhaitable de trouver des fonds qui permettraient de faire de la sensibilisation auprès des juges et des journalistes.

Alexander SEGER, Chef de la Division de la Cybercriminalité au sein du Conseil de l'Europe, explique :

- que la cybercriminalité menace les trois domaines d'activités du Conseil de l'Europe ;
- que des milliards de données sont volées ou bloquées et que moins d'1 % des cas sont poursuivis en justice.

En ce qui concerne la cybercriminalité, il est urgent de trouver des preuves de conspiration visant les attentats et éviter que plus d'enfants ne soient abusés (grooming).

Les Etats sont obligés de poursuivre en justice les infractions, et peuvent s'appuyer sur un « triangle » :

- la Convention 185 de Budapest et ses protocoles additionnels (auxquels se sont associés le Sénégal, l'Ile Maurice, le Canada, la République Dominicaine ainsi que les USA) qui « est le premier traité international sur les infractions pénales commises via l'Internet et d'autres réseaux informatiques, traitant en particulier des infractions portant atteinte aux droits d'auteurs, de la fraude liée à l'informatique, de la pornographie enfantine, ainsi que des infractions liées à la sécurité des réseaux. Il contient également une série de pouvoirs de procédures, tels que la perquisition de réseaux informatiques et l'interception ». Il définit les pouvoirs procéduraux ainsi que la coopération internationale ;
- le Comité de la Convention sur la Cybercriminalité qui regroupe les Etats Parties à la Convention et qui a pour but de faciliter l'usage et la mise en œuvre effective de la Convention, l'échange d'information et l'examen de tout futur amendement à la législation.

Mise en perspective

Sébastien FANTI, Avocat au Barreau valaisan (CH) et élu au poste de Préposé à la protection des données et à la transparence du Canton du Valais, est par ailleurs, membre de l'Union internationale des avocats (OING ayant le statut participatif auprès du Conseil de l'Europe, active dans un réseau d'avocats qui s'occupe de technologies avancées et de gouvernance internet). Il aborde le sujet en se prononçant clairement en faveur de l'éducation numérique des enfants et pour l'intégration de l'éducation à la robotique dans la vie quotidienne. Pour lui, il est temps de changer, de définir clairement ce que nous acceptons et ce qui n'est pas admissible. Nous avons le choix et ne devons pas rester à la merci des géants (Google, Microsoft et autres). Il faut essayer d'être pragmatique et protéger les droits des citoyens, mais également être vigilant et développer des réflexes de protection. Il faut fixer les limites, les garde-fous en matière de robotique, d'algorithmes, d'internet et prévenir les points de friction.

- Modifier les processus d'apprentissage pour les rendre cohérents avec l'utilisation effective et présumée (codage – plan « tuning »). Nos enfants doivent être incités à utiliser les outils du futur et non pas « Word », destiné à disparaître. L'apprentissage doit être modifié et compatible à ce que sera notre futur. Il est urgent que nous unissions nos forces pour éviter les doublons et pour renforcer les garde-fous. Nous ne savons pas où va s'arrêter le développement technologique (l'intelligence artificielle) et il faut d'urgence améliorer et favoriser les réflexions ;

- Ne devrait-on pas instaurer des e-procureurs qui pourraient être saisis « online » des plaintes et faire les rappels à la loi là où ceux-ci s'avèrent nécessaires ? On pourrait envisager une plateforme juridique de défense ;
- La « sex-torsion » et d'autres e-délits se font à partir de pays situés en Afrique et peu protégés ;
- Les règles arrivent trop tard (après que des milliards de données auront été volées, enregistrées et analysées à notre insu !) et nous ne devons pas attendre que quelque chose se passe mal pour agir.

Nous sommes responsables, avons le choix, et devons initier des changements. Il est nécessaire d'offrir aux citoyens un « statut numérique fort ». « La force d'une démocratie se mesure aux moyens des plus faibles et ce maillon n'a pas les moyens de se défendre pour le moment ».

Il faut une approche vertueuse, (p.ex., pour chaque robot qui remplacera une personne, il faudra proposer une formation via un fonds de reconversion). Sébastien Fanti pense que « le temps est venu pour le Conseil de l'Europe et les ONG qu'ils montrent la voie, initient le changement des pratiques nécessaires pour éviter que les êtres ne se qualifient par leur absence d'intégration à une société numérique qui, pour l'heure, génère des élites, mais néglige ses membres les plus vulnérables. Le temps est venu d'initier la courbe vertueuse qui rétablira l'égalité des chances et offrira à chacun les mêmes opportunités professionnelles et personnelles de profiter du progrès ! »

Nouvelles technologie, « privacy » et surveillance – perspective de l'organisation des droits de l'Homme

Jedrzej NIKLAS décrit la Fondation PANOPTYKON comme une ONG polonaise dédiée aux aspects droits de l'homme en lien avec le numérique. Cette ONG a pour but d'éduquer les citoyens à utiliser des outils de confidentialité lorsqu'ils utilisent internet et à leur faire prendre conscience des aspects légaux et éthiques en lien avec la technologie.

La technologie a deux facettes :

- Elle peut contribuer à soutenir/ protéger les droits de l'homme ;
- Elle peut avoir l'effet négatif de la surveillance. La grande majorité des citoyens n'est pas consciente de l'ampleur du phénomène de surveillance. Nous sommes contrôlés et catégorisés de plus en plus par de grandes firmes, qui détiennent un nombre incroyable d'informations à notre sujet. Il s'agit d'une intrusion à notre insu dans notre vie privée, pour contrôler nos vies et en tirer des données pour différentes raisons. Au début, surtout commerciales, mais de plus en plus pour des raisons de « sécurité publique », sous prétexte de « risk management », tout est 'monitoré', filmé, enregistré, du supermarché au parking, et souvent ailleurs ;
  Les algorithmes utilisés prennent des décisions sur nos vies. Les gens sont « catégorisés », ce qui affecte nos vies malgré nous. Je peux ne plus accéder à un site parce que les algorithmes m'ont calculé un certain profil. De nouveaux instruments sont développés. Les plus vulnérables sont les plus surveillés. Les migrants, p.ex., sont classés malgré eux dans une catégorie « seconde classe » plus surveillée. Cependant, les algorithmes peuvent se tromper. Aux Etats-Unis, il y a des gens qui sont considérés comme « suspects » suite à des erreurs de système. Ceci entretient un climat latent de méfiance et de peur. Ces « murs » qui se construisent masquent les vrais problèmes, mènent à des soupçons injustifiés et à un climat peu favorable à l'inclusion. Nous acceptons trop facilement de nous priver de liberté sans réfléchir aux conséquences réelles (Les caméras de surveillance n'ont jamais découragé ceux qui voulaient vraiment commettre un délit)

Nous devons donc nous engager pour une protection des données éthique

Echanges avec la salle:

- Question : Ne faut-il pas craindre que l'éducation numérique des enfants, l'avancée des technologies et l'intégration robotique dans la vie quotidienne mènent à la disparition progressive de la communication orale, de l'écriture et de la lecture ?
  Réponse : On n'a pas le droit de priver les enfants et les jeunes de se familiariser avec les technologies dont ils auront besoin dans la société d'information. Il faut donc inclure à tout prix l'opportunité d'apprendre sans pour autant supprimer les bases de communication classiques ;
- Les changements profonds de la façon dont est produite et consommée l'information appelle des réflexions spécifiques liées à la jeunesse et l'éducation. Les dimensions liées à la gouvernance d'internet et à la protection de la vie privée ne peuvent avoir un impact que dans la mesure où l'ensemble des citoyens, en commençant par les plus jeunes, sont outillés de manière adaptée pour affronter ces évolutions et ce nouvel environnement. Et pour le moment ils ne le sont pas. Les outils numériques sont censés donner une « égalité » des chances, mais nous ne sommes pas prêts à donner accès aux plus faibles. L'éducation (civique et citoyenne) doit prendre en compte les changements de la société et garantir l'éducation aux médias, l'éducation aux outils numérique, l'éducation à l'esprit critique et à ses outils. Dans le cadre d'un désengagement des Etats sur ces questions mais aussi d'un manque cruel d'innovation et de prise en compte de ces problématiques nouvelles, la responsabilité pèse hélas de plus en plus sur les associations, notamment celles qui portent des projets de jeunesse et d'éducation non-formelle. Cette réalité doit être rappelée et prise en compte dans le travail de la Conférence des OING qui doit s'engager dans un plaidoyer
- En termes d'actions concrètes, AEGEE / Association des Etats Généraux des Etudiants d'Europe (membre de la Conférence des OING) mène actuellement au niveau de l'Union Européenne, une Initiative Citoyenne Européenne pour un renouveau de l'éducation civique et citoyenne en Europe que l'ensemble de la Conférence est appelée à soutenir ;
- La société est profilée par « ce qu'on nous sert sur le net ». Il faut éviter l'exclusion sociale et envisager une approche holistique, qui inclut également la perspective théologique (cf. publication Eglise d'Ecosse)
- Il faut des logiciels libres coopératifs : travaillez en « open source », comme p.ex « Threma », pour un prix modique de 20 €. Méfiez-vous des clouds ;
- Il faut une vigilance pour protéger les citoyens face aux partis extrêmes. Le net ne doit pas être l'instrument des populistes qui divulguent un « racisme acceptable » à l'encontre de certains groupes de citoyens ;
- L'éducation à la pensée critique doit se fonder sur des capacités et sur les processus d'apprentissage collaboratifs… L'éducation ne va pas changer assez rapidement ;
- Il faut éviter l'utilisation abusive des données privées, que ce soit pour des raisons « commerciales » ou de contrôle par l'Etat. Les limites du pouvoir doivent être définies très clairement ;
- Le défi est colossal. Des aberrations et exagérations génèrent des dommages importants. Il faut aller vers un « abeas corpus numérique » qui permette d'avoir recours à une entité indépendante des Etats, un genre de « cour spéciale » qui permette aussi d'indemniser les victimes ;
- En vérité, aucun ordinateur ni aucune donnée ne permettra d'arrêter un terroriste ;
- Les lois sur la protection des données doivent pouvoir servir aux procureurs qui ne peuvent juger que sur base de lois ;
- Des solutions technologiques à la source ne seraient- elles pas plus efficaces que des lois ?

Les gouvernements doivent prendre des décisions responsables et éthiques, courageuses et fermes, concernant les outils acceptés/refusés (ex., Apple School est interdit dans les écoles en Suisse ; Windows 10 est interdit en Suisse ; Microsoft, a finalement accepté qu'au niveau mondial les processus doivent être contrôlés en « open source »). Les candidats aux élections doivent signer qu'ils acceptent les règles éthiques. Les Etats doivent d'urgence coopérer en vue de l'élaboration de bases légales communes. Les documents ne suffisent pas, il faut parvenir à une mise en œuvre des textes. Les OING doivent se mettre à l'avant-garde car elles ont un rôle très important.

En résumé

- Il est grand temps pour la société civile d'agir et de coopérer avec les Etats pour garder un équilibre respectueux des droits de l'homme. Ensemble, il faut collaborer avec les géants du numérique (Google, Facebook, Microsoft et autres) pour garantir et préserver nos droits. Il faut développer des comportements plus responsables et des réflexes de protection, fixer des limites, notamment en matière d'algorithmes, de robotique, renforcer les capacités et instaurer une e-plateforme juridique de défense du citoyen, et même, envisager une entité indépendante des Etats à laquelle on pourrait recourir en cas de dommage ;
- Les Etats doivent poursuivre en justice les infractions relevant de la cybercriminalité, même si ces infractions peuvent être « inconfortables » pour eux ;
- Il faut refuser la surveillance abusive sous prétexte de « risk management » ;
- Il faut une protection éthique des données qui ne nuit pas à l'inclusion des personnes vulnérables ni ne divulgue un « racisme acceptable » à l'encontre de certains groupes de citoyens ;
- L'ensemble des citoyens doit être outillé de manière adaptée pour affronter les évolutions et ce nouvel environnement. Une éducation numérique de qualité doit prendre en compte les changements de la société et garantir pour tous l'éducation aux médias, l'éducation à l'esprit critique et aux outils numériques pour rendre l'apprentissage compatible à ce que sera notre futur et garantir l'intégration à une société numérique qui ne néglige pas ses membres les plus vulnérables ;
- Il faut inciter les citoyens à utiliser des logiciels libres coopératifs pour travailler en « open source » ;
- La Conférence des OING se doit d'inclure ces questions dans ses travaux et ne manquera pas de rappeler aux gouvernements de prendre des décisions éthiques, courageuses et fermes.

Didier SCHRETTER, chargé de mission sur la communication et représentant de la Conférence des OING au Comité Directeur sur les Médias et la Société de l'Information (CDMSI) du Conseil de l'Europe, a remercié l'ensemble des intervenants pour le débat de qualité autour d'une problématique très complexe. Il a mis en perspective le lancement d'un débat plus large dans le cadre des travaux menés au sein de la Conférence des OING et des autres organes du Conseil de l'Europe. La société civile doit s'approprier les éléments qui suscitent des interrogations pour en débattre, faire les constats nécessaires et défendre avec détermination ses droits à la vie privée et à la liberté d'expression. Il a relevé la nécessité d'intégrer tous les aspects dans une approche globale ainsi que le besoin d'expertises pour agir de façon positive, créative et constructive, et a relevé la légitimité d'agir de manière courageuse en coopération avec tous les partenaires.