EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

Technologies et convention européenne

par Linos-Alexandre Sicilianos, président de la Cour européenne des droits de l'homme

Les auteurs d'un texte adopté en 1950 ne pouvaient tout simplement pas prévoir les évolutions technologiques qui ont eu lieu depuis, et moins encore leurs implications sur la Convention. Mais la Cour, en considérant la Convention comme « *un instrument vivant à interpréter (…) à la lumière des conditions de vie actuelles* » a certainement évité que ce texte ne devienne un « traité dormant », comme d'autres accords internationaux.

L'irruption des nouvelles technologies dans le droit de la Convention a eu des effets juridiques dans deux domaines tout à fait essentiels.

D'une part, pour tout ce qui concerne la liberté d'expression, protégée par l'article 10, et qui couvre aussi bien le droit de communiquer que celui de recevoir des informations. D'autre part, sous l'angle de la protection de la vie privée assurée par l'article 8.

Notre jurisprudence relative à ces deux dispositions est fortement marquée par les nouvelles technologies.

I. PARLONS D'ABORD DE LA LIBERTÉ D'EXPRESSION À L'ÈRE DES NOUVELLES TECHNOLOGIES

À l'heure à laquelle de plus en plus de citoyens s'informent principalement, voire pour certains exclusivement, et je pense aux plus jeunes, au moyen d'Internet, on ne sera pas surpris que des enjeux essentiels en matière de liberté d'expression se posent au regard de ce *« nouvel imaginaire qui domine nos sociétés »*, pour reprendre la formule d'Alain Supiot.

Dès 2012, la Cour a été amenée à observer que « *l'Internet est aujourd'hui devenu l'un des principaux moyens d'exercice par les individus de leur droit à la liberté d'expression et d'information* »[1].

Cette nouvelle forme de communication doit donc bénéficier, au même titre que les formes plus traditionnelles, de la protection assurée par la Convention européenne des droits de l'homme.

Linos-Alexandre Sicilianos

© JSS

Au niveau de la Cour, cette protection prend la forme d'un contrôle des ingérences de l'État dans l'exercice du droit garanti par l'article 10. Toutefois, l'article 17 prévoit aussi le cas où un individu abuse de ce droit, auquel cas il perd le bénéfice de la protection que la Convention accorde.

A. LES INGÉRENCES DE L'ÉTAT PEUVENT ÉVIDEMMENT PORTER ATTEINTE AU DROIT DE COMMUNIQUER ET DE RECEVOIR DES INFORMATIONS

La Cour en a très rapidement pris conscience s'agissant d'Internet, principalement dans des affaires concernant la Turquie et dans lesquelles les autorités de ce pays avaient décidé de bloquer l'accès des citoyens à des sites Internet, le plus connu internationalement étant le site YouTube.

Dans une de ces affaires, Cengiz c. Turquie de 2015, les requérants étaient des professeurs d'université qui se plaignaient de ne pas pouvoir accéder à ce site suite à son blocage par les autorités.

La position de la Cour a été claire : elle a affirmé que « *les sites Internet contribuent grandement à améliorer l'accès du public à l'actualité et, de manière générale, à faciliter la communication de l'information (...) La possibilité pour les individus de s'exprimer sur Internet constitue un outil sans précédent d'exercice de la liberté d'expression.* »[2]

Évidemment, à l'occasion de ce type d'affaires, quelle que soit la nature de l'ingérence en cause, notre Cour ne se contente pas de constater son existence. Elle examine les circonstances concrètes de l'adoption des mesures nationales et elle ne conclut à la violation de la Convention que si les conditions de légalité, de finalité et de nécessité ne sont pas satisfaites.

L'affaire Ahmet Yıldırım c. Turquie[3] a permis de préciser le sens de cette exigence en ce qui concerne le droit de recevoir des informations. Un tribunal avait bloqué l'accès à « *Google Sites* », car ce serveur hébergeait un site Internet dont le propriétaire faisait l'objet d'une procédure pénale. Cette mesure de blocage avait également pour effet de verrouiller l'accès à tous les autres sites hébergés par le serveur. Le requérant se plaignait de l'impossibilité d'accéder à son propre site Internet du fait de cette mesure ordonnée dans le cadre d'une affaire pénale qui n'avait aucun rapport ni avec lui, ni avec son site. Il voyait dans cette mesure une atteinte à son droit à la liberté de recevoir et communiquer des informations et des idées.

Outre cette condition de légalité, l'ingérence doit viser un but légitime, étant entendu que l'énumération des exceptions à la liberté d'expression figurant dans le second paragraphe de l'article 10 est exhaustive et que leur définition est restrictive.

Nous avons tous des difficultés à nous passer d'Internet, devenu une composante essentielle de notre droit à la liberté d'expression. Dans l'affaire Kalda c. Estonie[4] de 2016, un détenu se plaignait du refus des autorités de lui accorder un accès à trois sites Internet publiant des informations juridiques. Il soutenait que cette interdiction l'empêchait de mener des recherches juridiques.

La Cour a observé que les États ne sont pas tenus de fournir aux détenus un accès à Internet. Toutefois, lorsqu'un État accepte d'autoriser un tel accès – ce qui était le cas en Estonie –, il doit alors motiver son refus de donner accès à des sites spécifiques, ce qui n'avait pas été le cas, d'où le constat de violation de l'article 10.

Bien entendu, si la mesure nationale est conforme aux trois conditions prévues par la Convention,

1) CEDH, 18 décembre 2012, Ahmet Yildirim c. Turquie, n° 3111/10, § 54.
2) Cengiz et autres c. Turquie, arrêt du 1er décembre 2015, §§ 49 and 52.
3) CEDH, 18 décembre 2012, Ahmet Yıldırım c. Turquie, n° 3111/10.
4) CEDH, 19 janvier 2016, Kalda c. Estonie, n° 17429/10.

la Cour constatera la non-violation. Tel a été le cas, par exemple, dans l'affaire Delfi c. Estonie[5]. Il s'agissait de la première affaire de Grande Chambre dans laquelle la Cour était appelée à examiner un grief relatif à la responsabilité d'un portail d'actualités sur Internet en raison des commentaires laissés par les internautes.

Deux réalités contradictoires étaient au cœur de l'affaire : d'une part les avantages d'Internet que nous connaissons tous, notamment le fait qu'il constitue un outil sans précédent d'exercice de la liberté d'expression, d'autre part les risques qu'il présente, en particulier le fait qu'il permette que des propos haineux ou appelant à la violence soient diffusés dans le monde entier, en quelques secondes, et demeurent parfois en ligne indéfiniment. Autrefois, les médias classiques exerçaient un contrôle du contenu proposé au public. À l'heure d'Internet, ce contrôle, *a priori*, a disparu offrant a tout un chacun la possibilité de s'exprimer sans filtre avec les dérives que l'on constate parfois.

Pour trancher cette affaire délicate, la Cour a procédé à une appréciation *in concreto* des éléments pertinents. Ils l'ont conduit à juger que la décision des juridictions internes de tenir la société requérante pour responsable reposait sur des motifs pertinents et suffisants, et donc à conclure à la non-violation de l'article 10.

J'ajoute que l'arrêt Delfi est en phase avec la nécessaire responsabilisation des acteurs privés, dès lors que nous savons pertinemment que les acteurs publics ne sont absolument plus en mesure, dans nos sociétés de liberté, d'exercer le moindre contrôle *a priori* des opinions exprimées. Les questions que soulève cette affaire sont, je le sais, très présentes dans le travail que mènent les juges administratifs français.

Parfois, le requérant est déchu de son droit de se prévaloir de l'article 10.

Une telle possibilité découle de l'article 17 de la Convention, consacré à l'abus de droit. Son but général est, nous le comprenons tous ici, « *d'empêcher que des individus ou des groupements totalitaires puissent exploiter en leur faveur les principes posés par la Convention* ».

Les discours encourant une telle déchéance sont ceux qui menacent l'ordre démocratique, contiennent des propos négationnistes, des incitations à la haine raciale, religieuse ou sexuelle ou encore justifient la violence.

Or, incontestablement, les nouvelles technologies ont augmenté les risques de voir surgir de tels contenus dans l'anonymat et à l'abri de tout contrôle. Vous imaginez bien que la Cour, très fortement attachée à la liberté d'expression, ne fasse usage de l'article 17 qu'avec une extrême retenue, « *à titre exceptionnel et dans des hypothèses extrêmes* »[6].

La Cour a été contrainte d'y recourir dans l'affaire Belkacem c. Belgique[7] de 2017. Celle-ci concernait la condamnation du dirigeant de l'organisation « *Sharia4Belgium* » en raison de propos qu'il avait tenus dans des vidéos publiées sur YouTube. Le requérant appelait les auditeurs à dominer les personnes non-musulmanes à leur donner une leçon et à les combattre. La Cour n'a eu aucun doute quant à la teneur fortement haineuse des opinions du requérant. Elle a fait sienne la conclusion des tribunaux internes selon laquelle l'intéressé cherchait, par ses enregistrements, à faire haïr, à discriminer et à être violent à l'égard des personnes qui ne sont pas de confession musulmane. Estimant que le requérant tentait de détourner l'article 10 de sa vocation, elle a jugé qu'il ne pouvait bénéficier de la protection offerte par cette disposition et que sa requête devait être rejetée.

La protection de la vie privée, dont je vais parler maintenant, répond aux mêmes exigences.

II. J'EN VIENS DONC AUX MENACES QUE LES NOUVELLES TECHNOLOGIES FONT PESER SUR LA PROTECTION DE LA VIE PRIVÉE

Les juges européens ont, très tôt, pris la mesure des risques que les progrès technologiques pouvaient faire courir à la vie privée. En 2004, dans la célèbre affaire Von Hannover c. Allemagne[8], qui concernait des photos de la princesse Caroline de Monaco prises à son insu, la Cour rappelait la nécessité d'une « *vigilance accrue (…) face aux progrès techniques d'enregistrement et de reproduction de données personnelles d'un individu* ».

Tout comme pour la liberté d'expression, la protection de la vie privée est, essentiellement, assurée par un contrôle des ingérences de l'État. Toutefois, si parfois l'article 8 interdit aux autorités publiques certaines actions, il arrive également que cette disposition sanctionne certaines omissions.

Les ingérences des autorités publiques dans la vie privée des individus grâce aux nouvelles technologies sont multiples. Elles peuvent ainsi prendre la forme de perquisitions et de saisies des données électroniques dans le cabinet d'un avocat, de la conservation d'empreintes digitales dans un fichier électronique, de la décision d'un doyen d'université d'installer des caméras de surveillance dans les amphithéâtres, ou encore de l'établissement de différents régimes de surveillance, tels que l'interception massive des communications, le partage de renseignements avec des États étrangers et l'obtention de données de communication auprès de fournisseurs de services.

5) CEDH, 16 juin 2015, Delfi AS c. Estonie, GC., n° 64569/09
6) CEDH, 6 janvier 2011, Paksas c. Lituanie, GC, n° 34932/04, § 87.
7) CEDH, décision du 20 juillet 2017, Belkacem c. Belgique, n° 34367/14.
8) CEDH, 24 juin 2004, Von Hannover c. Allemagne, n° 59320/00.

Aussi variées que soient ces ingérences, dans tous les cas, le contrôle de la Cour porte sur la satisfaction des trois conditions posées par la Convention : légalité, finalité et nécessité que nous avons déjà rencontrées à propos de la liberté d'expression.

Pour être conforme à la Convention, l'ingérence doit donc, tout d'abord, être prévue par la loi. En ce domaine, le contrôle européen est minutieux, notamment quant à l'exigence de « prévisibilité » de la loi.

Il l'est singulièrement pour les mesures de surveillance secrète qui « *doivent se fonder sur une loi particulièrement précise* », permettant de tenir compte de la sophistication croissante de la technologie disponible.

Une affaire emblématique est certainement Roman Zakharov c. Russie[9] relative au système d'interception secrète des communications de téléphonie mobile en Russie.

Eu égard au défaut de recours au niveau national, ainsi qu'au caractère secret des mesures de surveillance et au fait que celles-ci touchaient tous les usagers des services de téléphonie mobile, la Cour a examiné la législation russe *in abstracto*.

Cet examen l'a conduit à considérer que les dispositions du droit russe régissant l'interception de communications ne comportaient pas de garanties adéquates et effectives contre l'arbitraire. Après avoir constaté des défaillances du cadre juridique dans un certain nombre de domaines, elle a conclu à la violation de l'article 8 de la Convention.

Tout récemment encore, il en a été de même dans l'affaire Ben Faiza c. France[10]. Celle-ci concernait des mesures de surveillance prises dans le cadre d'une enquête pénale portant sur un trafic de stupéfiants. La Cour a estimé que le droit français n'indiquait pas avec suffisamment de clarté l'étendue et les modalités d'exercice du pouvoir d'appréciation des autorités dans le domaine des mesures de géolocalisation.

L'ingérence doit, ensuite, viser un but légitime. Dans les affaires soumises à la Cour, l'atteinte à la vie privée opérée par les autorités publiques a pu être justifiée en vue de sauvegarder différents types d'intérêts publics.

Ainsi, dans l'affaire Uzun c. Allemagne[11], relative à la surveillance par GPS du requérant, il s'agissait d'enquêter sur plusieurs accusations de tentatives de meurtre revendiquées par un mouvement terroriste et la Cour n'a pas constaté de violation de l'article 8.

La protection des droits d'autrui doit également être prise en considération, par exemple ceux de l'employeur. Ainsi, dans l'affaire López Ribalda et autres c. Espagne[12], la Grande Chambre n'a pas constaté de violation de l'article 8 concernant la mise sous vidéosurveillance de caissières espagnoles sans que celles-ci en soient préalablement averties, malgré une obligation légale. La Cour a en effet jugé qu'une telle mesure était clairement justifiée en raison des soupçons légitimes d'irrégularités graves et des pertes constatées. Cette mesure de surveillance était proportionnée et légitime.

L'ingérence doit, enfin, être nécessaire dans une société démocratique. On retrouve ici le même contrôle de proportionnalité que celui opéré pour les atteintes à la liberté d'expression.

L'affaire S. et Marper c. Royaume-Uni[13] est emblématique. Elle concernait la rétention dans une base de données des empreintes digitales et données ADN des requérants après que les procédures pénales dirigées contre eux se furent soldées par un acquittement pour l'un et un classement sans suite pour l'autre.

« Les juges européens ont, très tôt, pris la mesure des risques que les progrès technologiques pouvaient faire courir à la vie privée ».

La Cour a jugé que le caractère général et indifférencié du pouvoir de conservation des données personnelles des individus soupçonnés mais non condamnés ne traduisait pas un juste équilibre entre les intérêts en jeu et elle a donc constaté la violation de l'article 8.

On peut citer également l'affaire de Grande Chambre Barbulescu c. Roumanie[14] qui concernait le licenciement d'un employé après que ses communications électroniques avaient été surveillées. La Cour a jugé que les autorités internes n'avaient pas protégé de manière adéquate le droit du requérant au respect de sa vie privée et n'avaient donc pas ménagé un juste équilibre entre les intérêts en jeu. Partant, elle a conclu qu'il y avait eu violation de l'article 8.

Une des affaires intéressantes de ces dernières années est certainement l'affaire M.L. et W.W. c. Allemagne[15]. Elle renvoie à ce phénomène d'hypermnésie collective que certains ont noté s'agissant d'Internet. Un phénomène dont le pendant est le droit à l'oubli revendiqué par certains. Chacun voudrait que l'on oublie ses erreurs et faiblesses passées. Or, Internet tend à rendre cela impossible. L'affaire concernait le refus de la Cour fédérale de justice d'interdire le maintien de l'accès à des dossiers de presse concernant la condamnation des requérants pour meurtre, sur les portails Internet de différents médias.

La Cour a rappelé que les médias ont pour mission de participer à la formation de l'opinion démocratique, en mettant à la disposition du public des informations anciennes conservées dans leurs archives. Elle a également rappelé que la manière de traiter un sujet relève de la liberté journalistique. Enfin, la Cour a relevé qu'au cours de leur dernière demande de révision du procès, les requérants s'étaient eux-mêmes tournés vers la presse à laquelle ils avaient transmis un certain nombre de documents tout en l'invitant à en tenir le public informé. La Cour a donc conclu à l'absence de violation de l'article 8, et a ainsi refusé aux requérants le « droit à l'oubli » qu'ils réclamaient.

Il est certain que tant la Cour européenne des droits de l'homme que les juridictions nationales seront, au cours des prochaines années, invitées à trancher des questions liées au déréférencement de liens figurant sur des moteurs de recherche et préjudiciables aux intérêts de personnes physiques. C'est une question d'une particulière importance pour le juge administratif français, comme cela résulte de la décision du Conseil d'État du 24 février 2017, qui consacre la compétence de la CNIL pour connaître des plaintes formées à la suite d'une décision de refus de déréférencement et ce, sous l'entier contrôle du juge administratif de l'excès de pouvoir.

Cette question témoigne de la proximité des missions du juge administratif français et du juge européen, illustration supplémentaire de notre responsabilité partagée pour la protection des droits et des libertés.

J'aurais pu citer ce matin bien d'autres exemples issus de notre jurisprudence, car celle-ci ne cesse de s'enrichir d'arrêts nés de l'apparition de ces nouvelles technologies, mais malheureusement le temps nous manque et il me faut conclure. […]

Chaque jour, nous constatons les progrès et les innovations que nous procurent les nouvelles technologies. En même temps qu'elles nous ouvrent sur le monde, elles bouleversent notre vie privée, nos relations de travail, notre droit à l'image ou à l'oubli. Bref, notre rapport au monde.

Mais nous ne pouvons plus nous en passer.

Les mutations qu'elles provoquent, les risques qu'elles font apparaître pour nos libertés, rendent indispensable l'intervention du juge, en tant que protecteur des droits fondamentaux.

Forte de ses 60 années d'expérience, la Cour de Strasbourg est prête à affronter ces nouveaux défis. L'appui des juges nationaux et notamment des juges administratifs français, dans le cadre de la subsidiarité, lui sera d'une aide précieuse et indispensable. C'est le message que je voulais porter ce matin devant vous.

2020-5718

9) CEDH, 4 décembre 2015, Roman Zakharov c. Russie, GC, n° 47143/06.
10) CEDH, 8 février 2018, Ben Faiza c. France, n° 31446/12.
11) CEDH, 2 septembre 2010, Uzun c. Allemagne, n° 35623/05.
12) CEDH, 17 octobre 2019, López Ribalda et autres c. Espagne, GC, n°1874/13 et 8567/13.
13) CEDH, 4 décembre 2008, S. et Marper c. Royaume-Uni, GC, n° 30562/04 et 30566/04.
14) CEDH, 5 septembre 2017, Barbulescu c. Roumanie, GC, n° 61496/08.
15) CEDH, 28 juin 2018, M.L. et W.W. c. Allemagne, n° 60798/10 et 65599/10.