

RECOMMANDATION N° 2018-01R

7 décembre 2018

COLLEGE DE DEONTOLOGIE

DES JURIDICTIONS FINANCIERES

Recommandation n° 2018-01R pour les personnels des juridictions financières sur le respect de la déontologie dans l'usage d'internet, des messageries et des médias sociaux

SOMMAIRE

PREAMBULE	p. 2
<i>Définitions</i>	
<i>Les développements d'internet, des messageries, des médias sociaux et des moteurs de recherche</i>	
<i>Le champ de la recommandation</i>	
I. ÉLÉMENTS DE DROIT	p. 3
A. Une pluralité de textes applicables	
1. Les textes généraux	
2. Les textes spécifiques aux juridictions financières	
B. Principaux éléments résultant des textes	
II. LES RISQUES SUR LESQUELS L'ATTENTION DES PERSONNELS EST APPELEE	p. 5
A. Une cartographie générale des risques	
1. Les risques absolus	
2. Les risques dont les conséquences déontologiques sont variables selon les cas (risques contingents) mais qui doivent être pris en compte en permanence.	
<i>a) Des risques déontologiques permanents tenant aux limites dans la sécurité des réseaux</i>	
<i>b) Des risques tenant au contenu-même des messages</i>	
B. Les éléments de modulation des risques contingents	
1. Les personnels concernés	
2. La probabilité du risque	
3. L'intensité du risque	
III. BONNES PRATIQUES D'USAGE	p. 8
A. Deux préconisations générales	
1. Une abstention totale de ce qui est caractérisé ci-dessus comme un risque absolu	
2. Un principe général de prudence dans les autres cas	
B. Exemples d'application	
1. Bonnes pratiques déontologiques dans l'utilisation des systèmes informatiques et des médias sociaux en elle-même	
<i>a) Pour éviter les conséquences déontologiques potentielles des risques intrinsèques tenant à la sécurité matérielle des systèmes et réseaux</i>	
<i>b) La traduction des principes déontologiques dans l'utilisation des systèmes</i>	
2. Bonnes pratiques concourant spécifiquement au respect de certains principes déontologiques	
<i>a) Secret et discrétion</i>	
<i>b) Neutralité, impartialité, respect du principe de laïcité</i>	
<i>c) Loyauté</i>	
<i>d) Dignité</i>	

PREAMBULE

Le Premier président a demandé au collège de déontologie de définir, au-delà des dispositions actuelles de la Charte de déontologie des juridictions financières, un cadre global et plus approfondi sur l'utilisation d'internet, des messageries et des réseaux sociaux et d'envisager le cas échéant de modifier ou compléter la Charte de déontologie.

Cette demande se situe dans un contexte de fort développement et de généralisation de l'usage de ces supports, à la fois dans la vie privée, dans la vie professionnelle et pour la vie publique. Même lorsqu'il relève de la liberté individuelle, cet usage peut avoir, en certains cas, des répercussions sur les juridictions financières et poser problème au regard des valeurs et principes déontologiques, comme la nécessité de ne pas porter atteinte à l'image et la réputation de ces juridictions. Le besoin existe pour les personnels eux-mêmes de disposer d'outils d'analyse et de repères.

Le collège a examiné les divers types actuels d'utilisation de ces vecteurs de communication et d'expression à la fois au plan des techniques utilisées et des pratiques sociales ainsi que leurs conséquences potentielles. Il a également analysé les textes, puis la jurisprudence et la doctrine qui se sont construites autour de ce sujet.

Définitions

Pour la formulation de la présente recommandation, le collège a retenu les définitions suivantes :

Internet est un système mondial et public d'interconnexion de réseaux informatiques qui permet à des ordinateurs et à des serveurs de communiquer efficacement au moyen d'un protocole de communication commun (IP). Il donne accès à des services virtuels dont les principaux sont le Web, le FTP, la messagerie et les groupes de discussion.

Les « médias sociaux » désignent plusieurs types d'applications Internet : les réseaux sociaux (Facebook, LinkedIn,), les blogs d'entreprise ou les microblogs (Twitter,), les sites web de partage de contenus multimédias (YouTube,...) et les wikis et autres outils de partage des connaissances. Leur finalité est donc la création, le développement et le maintien de relations sociales. Ils peuvent être ouverts à tous ou limités à un cercle qui peut lui-même être large ou restreint.

Une messagerie électronique sert à diffuser de l'information entre un émetteur et plusieurs destinataires ou à échanger de courts messages entre deux personnes (éventuellement avec copie à quelques autres), sans pour autant être le vecteur d'une communauté d'échanges. C'est une application utilisant internet, qui fonctionne en mode non connecté : le courrier est déposé dans une boîte aux lettres que le destinataire vient consulter lorsqu'il le souhaite.

Les développements d'internet, des messageries, des médias sociaux et des moteurs de recherche

La croissance de l'usage des réseaux sociaux et, plus largement, des médias sociaux, s'est traduite par une augmentation à la fois du nombre des utilisateurs, de la fréquence d'utilisation, du volume des informations échangées et par la diversification des vecteurs dans tous les champs de la vie professionnelle et de la vie privée. Ce phénomène concerne désormais la plupart des pratiques de lien social et de partage d'informations, la contribution aux débats et à la production d'idées et d'œuvres, mais aussi les offres et prestations de services.

Les progrès techniques considérables qui ont permis ces développements n'excluent pas la survenue de problèmes de sécurité dans la protection des informations diffusées, dont l'impact peut être majeur pour l'utilisateur même des médias sociaux considérés, voire pour les juridictions financières. Des processus de sécurisation des échanges et de garanties pour la protection et la fiabilité des données doivent donc être mis en place mais, en tout état de cause, l'état actuel des techniques ne permet pas de garantir une parfaite étanchéité des réseaux.

Par ailleurs, il existe en principe des médias sociaux à usage professionnel et d'autres à usage privé. Ils peuvent être soit dédiés à un cercle restreint, soit orientés vers une diffusion large voire publique ou quasi-publique. Dans la réalité, les interférences tendent cependant à se multiplier. Ainsi :

- La présence sur les médias sociaux est un élément de notoriété personnelle qui peut s'avérer utile, voire indispensable, pour le développement normal d'une carrière. Par exemple, certains médias sociaux considérés comme à vocation professionnelle servent à valoriser non seulement des réalisations professionnelles mais aussi l'image personnelle de l'utilisateur, certains aspects de sa vie privée, voire sa contribution à la vie publique.
- La possibilité existe qu'une messagerie professionnelle soit utilisée pour des messages à caractère personnel, soit par erreur, soit pour des raisons pratiques, soit encore parce que la frontière entre les deux sphères n'est pas toujours nette. Réciproquement, la messagerie personnelle est parfois utilisée dans une circonstance professionnelle.

Enfin, ces évolutions s'accompagnent d'une capacité exponentielle des moteurs de recherche pour rapprocher instantanément et permettre de croiser des informations tirées de sources de plus en plus diverses, sans distinction entre activités professionnelles et vie privée.

Le respect des valeurs et principes déontologiques suppose que l'usage d'internet, des messageries et des médias sociaux tienne compte de l'ensemble de ces circonstances de fait.

Le champ de la recommandation

Pour ce qui relève d'une recommandation, c'est-à-dire de conseils sur les bonnes pratiques de nature à favoriser le respect des valeurs et principes exprimés dans la Charte, le collège a donc rassemblé ci-après un ensemble de préconisations pour un usage éthique et prudent d'internet, des messageries et des médias sociaux. Elles visent à assurer, dans le contexte actuel, la protection des juridictions financières, mais aussi celle des utilisateurs eux-mêmes.

La présente recommandation s'adresse à l'ensemble des personnels de la Cour des comptes et des Chambres régionales et territoriales des comptes, qu'ils soient ou non couverts par la Charte de déontologie, pour fournir à tous et toutes des repères sur les précautions à prendre. Compte tenu de l'imbrication et des risques inhérents à l'utilisation des outils numériques, elle concerne l'utilisation de l'ensemble de ceux-ci, quelle qu'en soit la nature.

Le domaine numérique est par essence évolutif, mais il est possible de recenser les éléments de droit essentiels qui lui sont applicables, d'en déduire une cartographie des risques déontologiques sur lesquels l'attention doit être appelée et de dégager un ensemble de préconisations d'usage constituant des repères pour le respect des valeurs et principes déontologiques.

I. ÉLÉMENTS DE DROIT

Il existe une pluralité de textes applicables, dont résultent quelques conclusions générales.

A. Une pluralité de textes applicables

Les principales dispositions applicables sont, d'une part, des textes généraux et, d'autre part, des textes spécifiques aux juridictions financières.

1. Les textes généraux

[La Déclaration des droits de l'Homme et du Citoyen](#) (notamment ses articles 4, 10 et 11) et [la Convention européenne des droits de l'homme](#) (particulièrement son article 10)

[La loi du 29 juillet 1881 relative à la liberté de la presse](#), notamment ses dispositions en matière d'injures et de diffamation

[La loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés](#) et [le règlement général sur la protection des données \(RGPD\)](#), lequel encadre le traitement des données personnelles sur le territoire européen et crée des obligations pour les organismes qu'il définit

[La loi du 13 juillet 1983 portant droits et obligations des fonctionnaires](#), en particulier ses articles 25, 25 septies et 26

[La loi du 21 juin 2004 sur la confiance dans l'économie numérique](#), notamment pour ce qui concerne la lutte contre l'anonymat, et la [loi n° 2016-1321 du 7 octobre 2016 sur la République numérique](#), notamment ses articles 54 à 68

[Le code pénal](#), et notamment ses articles 225-1 et suivants, 226-1 et suivants, R.621-1 et -2, R.625-7 et suivants

[Le code civil](#), spécialement ses articles 7 à 15

[Le code de la propriété intellectuelle](#), en ses articles L.111-1 à L.112-4, L.331-1 à L.331-4, L.335-1.

2. Les textes spécifiques aux juridictions financières

[Le code des juridictions financières](#), en particulier ses articles L.120-3, L.120-5 et 6, L.220-4, L.220-6 et -7.

La [Charte de déontologie](#), notamment ses dispositions relatives à l'expression publique ainsi qu'à l'image et la réputation des juridictions financières, mais aussi les principes d'indépendance, de dignité et de loyauté, la neutralité et l'impartialité, les principes de comportement dans les relations avec les contrôlés et dans les relations professionnelles.

La [charte de bonne utilisation des ressources informatiques, d'internet et de la messagerie au sein du réseau des juridictions financières](#) de novembre 2011 (ci-après « charte informatique ») : instrument de « droit souple », elle vise à assurer la sécurité informatique des réseaux et de leurs applications en cas d'utilisation des ressources informatiques des juridictions financières et au sein de leur réseau. Elle aborde les différents éléments de cette sécurité et mentionne certains des risques déontologiques induits, même si, son objet n'étant pas de régler les questions déontologiques, elle n'en couvre pas tout le champ et ne concerne pas l'utilisation d'autres ressources et réseaux informatiques que ceux des juridictions financières.

B. Principaux éléments résultant des textes

Sans entrer dans une analyse détaillée de ces textes, quatre éléments principaux en ressortent :

- Dans leur globalité, ils garantissent une libre circulation des idées et la liberté d'expression des personnes mais encadrent l'exercice de ces libertés.
- Sauf exception, ils ne visent aucun moyen de communication en particulier mais sont susceptibles de concerner l'ensemble des moyens numériques. Ils s'attachent à caractériser les conditions et l'étendue de l'atteinte à un droit ou à une liberté garantis, voire des cas de manquement déontologique, ainsi que les sanctions encourues.
- Ils concernent les citoyens eux-mêmes, dans l'exercice de leur liberté d'expression, mais ils valent aussi pour leur vie professionnelle. Dans le cadre professionnel, ils sont susceptibles de produire des effets également sur l'employeur : en effet, la responsabilité de ce dernier peut être recherchée pour des faits ou actes imputables à ses agents et non dépourvus de tout lien avec leurs fonctions.
- Ils énoncent ou renforcent, pour les juridictions financières ou certains de leurs personnels,

des obligations qui n'existent pas dans les services administratifs (principe d'indépendance) ou pas au même degré (obligation de réserve, qui, dans le cas général, ne résulte que d'une construction jurisprudentielle), voire qui ne sont pas prévues pour certaines autres juridictions (prestation d'un serment).

Ces points doivent d'autant plus être relevés que, comme indiqué précédemment, une porosité croissante existe entre les moyens et supports de communication accessibles à tous et les moyens et supports privés, ainsi qu'entre les utilisations professionnelles et privées.

II. LES RISQUES SUR LESQUELS L'ATTENTION DES PERSONNELS EST APPELÉE

De la pluralité des textes et des situations se dégage une pluralité de risques déontologiques. La nouveauté de ces sujets et l'usage de plus en plus constant des vecteurs numériques dans la vie professionnelle et personnelle conduisent à appeler en premier lieu l'attention de l'ensemble des personnels sur plusieurs éléments de cartographie des risques et de modulation de leur intensité.

A. La cartographie générale des risques

L'utilisation des vecteurs concernés présente deux grandes catégories de risques, qui valent pour les usages aussi bien professionnels que personnels. La gradation des risques conduit en effet à identifier d'une part des risques par nature inacceptables, et d'autre part des risques dont les conséquences déontologiques éventuelles sont à apprécier en fonction des circonstances. Cette cartographie tire notamment les conséquences, au plan de la déontologie, des risques cités dans la charte informatique.

1. Les risques absolus

Certains risques vont par nature à l'encontre des valeurs et principes déontologiques, sans qu'il soit nécessaire d'entrer dans une analyse des circonstances.

Il en est ainsi pour les messages qui porteraient atteinte à des principes ou à des droits constitutionnellement reconnus et garantis, par exemple par la Déclaration des droits de l'homme et du Citoyen. La Cour et les CRTC étant des juridictions et jouant un rôle dans le fonctionnement des institutions, il en est de même pour ceux qui iraient à l'encontre des principes fondamentaux d'une juridiction ou mettraient en cause les institutions.

Il en est également de même pour les atteintes au droit à l'image et à la vie privée, régies par le code civil et le code pénal.

Compte tenu de leur nature, ces comportements constituent un risque inacceptable pour les juridictions financières : ils peuvent porter atteinte tant à l'image et à la réputation de ces dernières qu'à de nombreux principes et valeurs exprimés dans la Charte de déontologie, tels, selon les pratiques concernées, la dignité, la loyauté, la neutralité, l'impartialité ou l'indépendance.

Bien entendu, constituent a fortiori des risques absolus les utilisations de tout vecteur numérique pour des pratiques pénalement réprimées comme la diffusion de propos incitant à la haine raciale, d'images violentes ou pédophiles, le harcèlement ou l'apologie du terrorisme. La retransmission de tels messages présente un risque assimilable.

Le risque existe quel que soit le vecteur de communication ou de diffusion utilisé. Dans le cas des vecteurs numériques, certains éléments, comme le caractère public de l'atteinte ou l'élément intentionnel, peuvent être plus complexes à analyser et à prouver que lorsque sont utilisés des vecteurs traditionnels comme la presse écrite, mais le risque déontologique est de même nature.

En matière, par exemple, d'injures et de propos diffamatoires sur les réseaux sociaux, les juridictions civiles, avec le développement des réseaux d'« amis » et des sites d'intérêts partagés, se sont montrées attentives à protéger le droit d'expression privé. Certes, elles ont jugé qu'à l'intérieur d'un site accessible aux seules personnes agréées par le titulaire, en nombre restreint, les propos même injurieux, sont privés. La Cour de cassation a confirmé cette position (Cass., 1re chambre civile, 10 avril 2013, n° 11-19.530). En revanche, dans d'autres types de cas, des juridictions prud'homales et administratives (CA de Reims 9 juin 2010) mais aussi le Tribunal de grande instance de Béthune (14 décembre 2010) ont considéré que des publications sur des réseaux comme Facebook, les blogs et autres sites internet, qui n'offrent pas toutes les garanties de confidentialité, n'assurent pas en conséquence toute la discrétion nécessaire pour des propos censés rester dans la sphère privée. Or, dans la pratique, l'utilisateur recherche souvent une diffusion plus large que son seul cercle de relations proches et, en tout état de cause, la limitation effective de la diffusion ne peut être garantie en l'état actuel de la sécurité et du mode de fonctionnement des systèmes.

2. Les risques dont les conséquences déontologiques sont variables selon les cas (risques contingents) mais qui doivent être pris en compte en permanence

Une deuxième catégorie concerne les risques déontologiques qui doivent être appréciés en tenant compte de différents éléments de fait. Ils peuvent être induits soit par les limites de la sécurité sur internet, les messageries et les médias sociaux, soit par le contenu même des messages diffusés. S'ils doivent être examinés au cas par cas, ils peuvent exister lors de toute utilisation.

a) Des risques déontologiques permanents tenant aux limites dans la sécurité des réseaux

Il peut s'agir d'un risque de divulgation tenant à des tiers, par exemple par intrusion dans les systèmes (notamment par appropriation d'un mot de passe, utilisation des failles du réseau pour en capter des données ou messages, décryptage des systèmes de chiffrement utilisés par un réseau). Des failles techniques ou des possibilités d'intrusions sont constatées de plus en plus souvent, quelles que soient les protections mises en place. Il existe des moyens techniques de plus en plus offensifs pour casser les codes de confidentialité. En outre, les constructeurs, les opérateurs et les fournisseurs d'applications ont la maîtrise de certains éléments de paramétrage, sans que l'utilisateur en ait toujours connaissance ou la possibilité de les modifier pour se protéger.

Ce type de risques peut être aggravé par la conservation de données, qu'il s'agisse de textes ou d'images. Sur internet et en particulier sur les réseaux sociaux, l'oubli numérique n'existe pas. Tout ce qui est publié ou partagé sera difficilement effaçable. Ainsi l'archivage illimité des données tout comme les possibilités de recherches nominatives peuvent permettre de rendre publiques, à terme proche ou lointain, des éléments de la vie personnelle ou des opinions privées.

L'attention doit être particulièrement attirée sur la possibilité, pour les internautes, d'opérer de plus en plus facilement des rapprochements et croisements avec d'autres informations accessibles sur internet. Un même utilisateur détient en général simultanément plusieurs comptes professionnels ou à la fois des comptes professionnels et personnels. Même si seul l'un d'entre eux mentionne l'appartenance aux juridictions financières, les moteurs de recherche permettent à des tiers de faire un rapprochement instantané entre tous les comptes et profils de l'utilisateur. Le risque est par exemple que le croisement d'informations conduise à considérer qu'il y a atteinte au principe de neutralité ou à l'obligation de réserve.

Le risque peut par ailleurs être aggravé par les adhésions « en cascade » : l'adhésion à un site ou une application s'accompagne de plus en plus, à l'insu de l'utilisateur, d'une adhésion imposée à d'autres sites ou applications.

b) Des risques tenant au contenu-même des messages

Ces risques au regard des dispositions déontologiques récapitulées au I. peuvent se manifester dans de nombreuses circonstances et dès lors que des vecteurs numériques sont utilisés :

- *dans l'exercice des diverses activités* : l'activité principale lorsqu'une messagerie ou un média social y est utilisé, mais aussi, en raison des risques de porosité, dans les activités accessoires, voire certaines activités privées. L'activité principale exercée en dehors de la juridiction (détachement, disponibilité...) peut également être concernée, même si c'est à un degré moindre, ainsi que le cas où, après son départ à la retraite, l'agent exerce encore des fonctions au titre de la Cour ou des CRTC.

- *par tout vecteur* : un message électronique, un « tweet », un blog ou autres inscriptions sur les « murs » (Facebook),... L'atteinte peut naître de toute diffusion, même de l'envoi à un nombre de destinataires initialement très limité, en raison des risques de reproduction et de diffusion non maîtrisées, par des tiers, de tout ou partie des contenus diffusés (via des « transferts » ou des « partages » par exemple).

B. Les éléments de modulation des risques contingents

Lorsqu'il s'agit de risques contingents, dont les conséquences déontologiques sont à apprécier au cas par cas, il convient de prendre en compte notamment la probabilité du risque et son intensité.

1. Les personnels concernés :

Plusieurs risques d'atteinte aux principes déontologiques concernent l'ensemble des personnels :

- Le risque d'atteinte aux principes consacrés par l'article 25 de la loi n° 83-634 : la dignité, l'impartialité, l'intégrité et la probité, la neutralité et le principe de laïcité ;
- Le risque d'atteinte au secret professionnel et à la discrétion professionnelle (article 26 de cette même loi)¹.

Certains risques concernent plus particulièrement une partie des personnels :

- Le devoir de réserve spécifiquement affirmé (articles L. 120-5 et 220-6 du CJF) pour les « membres » des juridictions financières, c'est-à-dire, au sens des textes, les magistrats : tout membre de la Cour des comptes ou des CRTC « s'abstient de tout acte ou comportement à caractère public incompatible avec la réserve que lui imposent ses fonctions ». Ces mêmes articles sont applicables, pendant l'exercice de leurs fonctions dans les juridictions financières, aux personnels mentionnés aux sections 2 à 5 du chapitre II du titre Ier livre 1er (CMSE, CRSE, rapporteurs extérieurs, conseillers experts) et à l'article L. 212-7 ainsi qu'aux vérificateurs des juridictions financières.
- Les risques inhérents à la mention de l'appartenance aux juridictions financières (mêmes articles L. 120-5 et L. 212-7 CJF) : aucun membre de la Cour ou des CRTC ne peut se prévaloir, à l'appui d'une activité politique, de (cette) appartenance. Il en est de même pour les personnels des sections 2 à 5 du chapitre II du titre Ier et de l'article L. 212-7 pendant l'exercice de leurs fonctions.
- Les principes de dignité et de loyauté valent pour tous les personnels, mais leur portée se trouve renforcée pour ceux qui prêtent serment, et a fortiori s'ils sont soumis à la Charte de déontologie et si leur serment est, aux termes du CJF, définitif.
- Pour les personnels soumis à la Charte de déontologie, l'atteinte à l'image et à la réputation des juridictions financières, principe énoncé au point 4 de cette Charte.

¹ L'avis du collège n°2010-04 du 28 octobre 2010 insistait déjà sur les obligations de secret et de discrétion professionnels dans l'utilisation des nouvelles technologies de l'information et de la communication « Réflexions sur l'applicabilité des obligations de secret -et de discrétion professionnels des magistrats des juridictions financières à l'utilisation des nouvelles technologies de la communication ». Sur cet avis cf. aussi *infra* III.B.2. Loyauté.

2. La probabilité du risque

- *La distinction entre usage professionnel et personnel :*

Les interconnexions potentielles entre réseaux et messageries privés et professionnels relativisent la portée de cette distinction en termes de risques et accroissent la probabilité de ceux-ci (Conseil d'Etat, 27 juin 2018, n°412541).

- *La distinction entre une participation active ou une présence passive sur les réseaux :*

Le risque est évidemment plus fort dans le premier cas. Cependant, même une présence passive, se limitant à la consultation ou conservation des informations reçues sans émettre soi-même de messages, peut exposer à certains des risques analysés ci-dessus.

- *Le nombre des « correspondants », « relations » ou « amis » sur les réseaux, ou de destinataires des messages :*

Un nombre élevé majore le risque de divulgation d'informations ou de données. Certains risques tiennent à l'acceptation des « amis » ou « contacts », car les médias sociaux sont utilisés pour échanger avec des relations existantes mais aussi pour élargir le cercle des relations. Or, par l'entrée dans un réseau d'« amis », le tiers accède à des informations jusqu'alors protégées. Une « relation » inscrite dans un réseau pourra, nonobstant l'absence d'accord de son émetteur initial, divulguer beaucoup plus largement une information qui lui a été communiquée *via* le réseau.

3. L'intensité du risque

- *Le positionnement hiérarchique, la nature des fonctions et la notoriété individuelle de l'émetteur n'ont pas nécessairement d'impact sur la probabilité du risque mais peuvent influencer sa portée. Ils sont en effet susceptibles d'aggraver les conséquences d'un éventuel manquement pour les juridictions financières. Cependant, l'atteinte à l'image et la réputation de celles-ci peut toujours exister et doit toujours être prise en compte.*
- *Le risque est encore plus fort pour les personnels qui, par les contrôles auxquels ils participent et les documents auxquels ils ont accès, ont connaissance de données sensibles, par exemple en matière de défense, de fonctionnement des pouvoirs publics ou d'entreprises soumises au contrôle des juridictions financières. Ce risque justifie des précautions particulières, notamment dans l'acceptation de demandes d'entrée en relation sur leur(s) réseau(x) privé(s) et dans la diffusion de contenus.*
- *Le recours à des pseudonymes ne réduit qu'apparemment l'intensité du risque car des possibilités techniques existent de ré-identification de l'auteur réel des envois réputés anonymisés (sur ce recours, cf. aussi infra III. B. 2. Loyauté).*

III. BONNES PRATIQUES D'USAGE

Outre l'attention aux risques à laquelle ils appellent, les éléments ci-dessus conduisent à recommander aux personnels des juridictions financières un ensemble de bonnes pratiques. Celles-ci visent, même si elles ne sont pas exhaustives, à leur fournir des repères pour les aider à respecter les valeurs et principes déontologiques qui sont un élément essentiel de l'image et de la réputation des juridictions financières et une condition de la confiance accordée à celles-ci.

A. Deux préconisations générales

Dans l'usage qu'ils font d'internet, des messageries et des médias sociaux, les magistrats et personnels des juridictions financières prennent en compte les valeurs et principes déontologiques et appliquent des précautions proportionnées au type de risques.

1. Une abstention totale de ce qui est caractérisé ci-dessus comme un risque absolu

Il s'agit en effet d'actes ou de pratiques prohibés par les textes et/ou d'une particulière gravité.

2. Un principe général de prudence dans les autres cas

L'ensemble des analyses qui précèdent amène à formuler un principe général de prudence :

La prolifération des usages d'internet, la porosité des espaces privés et publics sur les médias et messageries numériques et la puissance des moteurs de recherche justifient que chacun applique dans ses fonctions mais aussi dans ses utilisations privées, un principe général de prudence au cours de toute navigation sur ces espaces. Ce principe comporte à la fois une vigilance dans l'usage, une retenue dans les comportements et une modération dans les contenus. Il constitue un repère permanent sur l'ensemble des vecteurs numériques, que les moyens utilisés soient ceux des juridictions financières ou des moyens privés et qu'il s'agisse d'usages professionnels ou personnels.

B. Exemples d'applications.

Le principe de prudence vise à prévenir par de bonnes pratiques l'ensemble des risques déontologiques, y compris ceux liés à la sécurité des systèmes informatiques et des médias sociaux.

1. Bonnes pratiques déontologiques dans l'utilisation des systèmes informatiques et des médias sociaux en elle-même :

a) Pour éviter les conséquences déontologiques potentielles des risques intrinsèques tenant aux insuffisances dans la sécurité matérielle des systèmes et réseaux.

Les dispositions pratiques figurant dans la charte informatique peuvent être considérées comme concourant au respect par tous les personnels des principes déontologiques. Elles peuvent constituer des repères pour les utilisateurs même en dehors de leur champ spécifique, l'utilisation des systèmes des juridictions financières, et valoir pour l'usage de systèmes, vecteurs et réseaux extérieurs à ceux de ces juridictions. On peut en déduire par exemple les points suivants :

- Les paramètres de confidentialité doivent être choisis de façon à sécuriser au maximum l'usage du compte, même privé, et **il est préférable de choisir pour les comptes privés des paramètres différents de ceux retenus pour les comptes professionnels.**
- **La mise en ligne sur un site professionnel d'informations privées ou de liens vers des profils privés est à éviter** : elle peut accentuer la vulnérabilité de l'ensemble des comptes et données qui y sont hébergées et par ricochet celle des proches, mais aussi de l'Institution.

b) La traduction des principes déontologiques dans l'usage des systèmes numériques

Les précautions liées à la sécurité matérielle et technique du système, des applications et des supports des juridictions financières relèvent des dispositions d'organisation de celles-ci. La charte informatique, en son article 5, cite diverses opérations anormales et demande aux utilisateurs de s'en abstenir². Ces prescriptions touchent aux devoirs de loyauté et de probité et valent aussi pour les usages privés.

² Par exemple, veiller à ne pas altérer ou détruire des matrices ou supports d'application, ne pas perturber le fonctionnement normal du réseau ou l'utiliser de façon déloyale dans le but de le détourner à des fins personnelles ; de même ne pas détourner ou détruire les informations présentes dans un système ni l'utiliser d'une manière abusive ; pour se connecter sur un site ou un appareil informatique, y être autorisé et avoir obtenu les codes d'accès et d'identification de manière légale ; ne pas usurper l'identité d'autrui, ni s'approprier les mots de passe d'autres utilisateurs.

Une vigilance est en outre particulièrement conseillée sur deux points :

- *Des précautions pour séparer les utilisations professionnelles et privées* : l'utilisation directe de l'adresse professionnelle pour un usage à caractère personnel et privé est à éviter. Le **nom, le logo ou une image des juridictions financières ne peuvent pas être mentionnés** pour la création d'un compte personnel ou apparaître dans son utilisation.
- *Le discernement dans la sélection des contacts et l'adhésion aux multiples sites et applications qui sont proposés* : le fonctionnement en réseaux étant d'essence participative, l'utilisateur peut être considéré comme membre actif d'un processus contractuel d'échanges. Il fournit du contenu accessible à d'autres, publiquement ou de manière privée. Il peut ainsi être regardé comme participant au fonctionnement du ou des réseaux dont il est adhérent et peut à ce titre voir sa responsabilité engagée. Il est dès lors conseillé de **n'accepter sur les réseaux personnels que des personnes connues ou sur lesquelles il est possible de disposer d'informations fiables**. Outre les paramétrages du compte, il convient de **ne pas hésiter à recourir aux fonctionnalités « supprimer » ou « bloquer »** à l'encontre d'un membre d'un groupe dont on est administrateur.

2. Bonnes pratiques concourant spécifiquement au respect de certains principes déontologiques

Sans prétendre à l'exhaustivité, le domaine du numérique étant protéiforme et fortement évolutif, les pratiques suivantes peuvent concourir au respect des valeurs et principes déontologiques. La retenue dans le comportement et la modération dans les contenus et la portée des messages sont d'autant plus à observer lorsqu'une personne utilise plusieurs réseaux et s'adresse à des correspondants diversifiés et pouvant appartenir à des communautés d'intérêts diverses.

a) Secret et discrétion

Le **compte d'un réseau social** doit être regardé par son utilisateur, qui y agit en tant qu'éditeur de contenu, comme relevant par principe de l'espace public. Les personnels des juridictions financières qui entendent à titre personnel être présents sur des médias sociaux doivent dès lors respecter l'obligation de réserve, le secret professionnel, le secret du délibéré et la discrétion professionnelle, quels que soient le réseau social, les paramétrages utilisés ou le nombre de contacts du titulaire du compte (CE 20 mars 2017, n° 393320).

Ces obligations comportent celle de respecter la confidentialité des informations auxquelles l'utilisateur a accès ou qu'il gère. Si ce dernier point est spécifiquement rappelé aux magistrats, rapporteurs et autres personnes concernées dans la Charte de déontologie (articles 4, 27, 34, 36), il s'impose à l'ensemble des personnels des juridictions financières.

b) Neutralité, impartialité, respect du principe de laïcité

Si, dans un souci de transparence, le **profil professionnel** doit être exact, il est conseillé de n'utiliser qu'avec retenue l'appartenance aux juridictions financières et la qualité de magistrat ou d'agent de la Cour des comptes ou des CRTC. Si une telle mention va de soi sur les réseaux à vocation professionnelle, c'est sous réserve que l'utilisateur reste vigilant sur les contenus qu'il publie, sur la sélection de ses contacts et sur les échanges directs ou indirects qu'il entretient avec ceux-ci.

Une proportionnalité est souhaitable entre la description de l'utilisateur faite dans le profil et la nature des informations diffusées sur le site.

Une **messaging** autre que celle des juridictions financières doit en principe être employée pour tout usage privé (cf. supra) et la différenciation doit être assurée autant que possible entre les usages professionnels et personnels. En cas d'adhésion à des réseaux à vocation professionnelle (LinkedIn,

Viadeo...) il est préférable, dans le cas général, d'éviter que le profil mette en avant l'appartenance aux juridictions financières ; lorsque l'adhésion vise à permettre de diffuser seulement des informations au titre de l'institution, cette mention ne présente pas les mêmes risques.

Si l'appartenance³ aux juridictions financières apparaît dans le profil, le principe de prudence trouve d'autant plus à s'appliquer et limite les possibilités d'expression. Les réseaux pouvant conserver indéfiniment la « mémoire » des informations diffusées, il paraît de sage pratique de mettre de préférence en avant une fonction accessoire ou ancienne en cohérence avec le domaine d'intervention choisi. Il convient cependant d'avoir conscience des limites de cette précaution et, en conséquence, la modération des propos est en tous les cas recommandée.

L'expression des opinions, croyances religieuses, philosophiques ou politiques est à cantonner à l'espace privé, pour ne pas risquer de porter atteinte aux principes de neutralité, d'impartialité et de respect de la laïcité. Les risques particuliers des supports numériques rendent souhaitable la modération dans cette expression.

c) Loyauté

Dans les usages professionnels ou dans tous ceux qui sont susceptibles de concerner directement ou indirectement les juridictions financières, l'utilisateur ne masque pas son identité. Il n'utilise pas de pseudonyme lorsqu'un tel recours viserait à lui permettre de s'affranchir du respect des valeurs et principes exprimés dans la Charte ou d'autres obligations déontologiques.

L'expression d'opinions personnelles étrangères à l'activité professionnelle est à écarter sur les réseaux des juridictions financières. L'est aussi l'expression susceptible de leur porter préjudice.

Lorsque les personnels des juridictions financières commentent sur des médias sociaux l'actualité juridique et administrative, ils doivent faire preuve non seulement de modération dans les propos qu'ils tiennent mais d'une vigilance équivalente à celle qu'impliquerait leur publication.

Toutes initiatives d'expression dans les médias sociaux ne doivent pas interférer avec la politique de communication des juridictions financières. L'obligation de loyauté envers l'institution se combine ici avec celle de discrétion. Les propos ou commentaires faisant référence à des événements professionnels, à des décisions prises par l'Institution et singulièrement aux activités ou missions exercées par le titulaire du compte sont à éviter, sauf accord de l'autorité hiérarchique⁴.

d) Dignité

Au-delà des aspects précédemment évoqués au titre notamment de la sécurité, la retenue dans le comportement et la modération dans les contenus des messages et échanges sont des conditions du respect du principe de dignité.

*

Certains des points qui précèdent mériteraient, compte tenu de leur portée générale, d'être traduits dans la Charte de déontologie elle-même, notamment le principe général de prudence (cf. III.A.2.).

La vigilance sur les risques et le respect, par tous les personnels, des bonnes pratiques dans l'usage d'internet, des messageries et des médias sociaux, concourront à la fois à la protection de chacun et à la préservation de l'image et de la réputation des juridictions financières.

³ Deux points de la Charte sont à retenir : le point 14 « (...) les personnes concernées (...) dans le cadre de leurs activités politiques, philosophiques ou confessionnelles, (...) ne mettent pas en avant leur appartenance à l'institution ou leur collaboration aux travaux de celle-ci » ; le point 32 « Dans les messages qu'elles envoient sur les réseaux sociaux ou sur les messageries non professionnelles, elles ne font pas état de leur appartenance aux juridictions financières ».

⁴ Le collège de déontologie a considéré dans son avis n° 2010-04 du 28 octobre 2010 précité que cet accord doit être obtenu préalablement à « la diffusion d'informations ou de commentaires sur l'activité des juridictions financières ».