

La protection des données sur Internet en droit suisse

Michel JACCARD(*)

Lex Electronica, vol. 6, n°2, Hiver / Winter 2001

Synopsis

Internet data protection in Switzerland can trace its sources to the State constitution and a federal law adopted long before the Internet ever existed. The legislation in question is coupled with Switzerland's international commitments, notably the *European Convention on Human Rights of the Council of Europe*.

To begin, this article focuses on how the legislation on Internet data protection applies to people and State authorities which deal with personal information data banks. Secondly, this article analyses the fundamental principles behind the legislation (legalities, good faith, proportionality, finality, exactitude, foreign communication, security and freedom of access) and their application to Internet. Lastly, the protection of e-mail content is briefly discussed in the context of recent jurisprudence and in perspective of telecommunication privacy.

Résumé

La protection des données personnelles en Suisse trouve son fondement dans la constitution et se concrétise avant tout dans une loi fédérale adoptée avant l'avènement d'Internet et la généralisation de la transmission d'informations personnelles sur des réseaux numériques. Cette réglementation est complétée par les engagements internationaux de la Suisse et notamment la *Convention européenne des Droits de l'Homme du Conseil de l'Europe*.

L'article délimite tout d'abord le champ d'application de la législation, qui joue un rôle pour le traitement de données personnelles par des particuliers comme par les autorités de l'administration fédérale. Suit une brève analyse des principes fondamentaux (licéité, bonne foi, proportionnalité, finalité, exactitude, communication à l'étranger, sécurité, droit d'accès) et de leur application sur Internet. Enfin, la protection du contenu des messages électroniques privés est brièvement abordée sous l'angle du secret des télécommunications et à la lumière d'une jurisprudence récente du Tribunal fédéral.

Table des matières

A. En général

B. Les principes de la protection des données au plan fédéral

1. Le siège de la matière
2. Les principes matériels du traitement des données dans la LPD
3. Le traitement des données par des personnes privées (art. 12 à 15 LPD)
4. Le traitement des données par des organes fédéraux (art. 16 à 25 LPD)
5. Le préposé fédéral à la protection des données (art. 26 à 32 LPD)
6. Sanctions pénales (art. 34 et 35 LPD)
7. Secret des télécommunications

Conclusion

Bibliographie

A. En général

1. La protection des données en Suisse est en premier lieu assurée par l'art. 13 al. 2 de la nouvelle Constitution fédérale, entrée en vigueur le 1^{er} janvier 2000 (RS 101), en vertu duquel "*toute personne a le droit d'être protégée contre l'emploi abusif des données qui la concernent*".

2. Au plan fédéral, une réglementation homogène s'applique aux relations entre particuliers et autorités fédérales ainsi qu'aux rapports horizontaux entre particuliers (voir *infra* B). Fédéralisme oblige, les cantons et demi-cantons restent pourtant compétents pour édicter une réglementation spécifique qui traiterait des relations entre particuliers et autorités cantonales et communales. Dans la mesure où ces réglementations ne sont toutefois pas uniformisées, même si elles doivent respecter les principes constitutionnels, elles ne seront pas étudiées.

3. Par ailleurs, quelques dispositions éparses du droit fédéral offrent une protection spécifique dans des domaines particuliers. On peut par exemple penser au régime spécifique dont jouit la presse[1], les banques[2] ou des professions comme les avocats, les hommes d'Église ou les médecins[3]. Faute de place, ces disparités ne seront pas étudiées.

Enfin, le secret des télécommunications peut jouer un rôle important en matière d'Internet (voir *infra* B.7).

4. À cette réglementation interne s'ajoutent les conventions internationales auxquelles la Suisse a adhéré et qui ne nécessitent pas, de manière générale, de transposition formelle en droit interne. Il s'agit notamment de l'art. 8 de la *Convention européenne des droits de l'Homme* du 4 novembre 1950 (CEDH, RS 0.101)[4]. Plus récemment le Conseil de l'Europe, dont la Suisse fait partie, a adopté le 28 janvier 1981 une Convention (n° 108) pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel[5], ainsi qu'une Recommandation R (99)5 du 23 février 1999 sur la protection de la vie privée sur Internet[6], dont le Juge suisse s'inspirera certainement s'il doit se prononcer sur ces questions.

B. Les principes de la protection des données au plan fédéral

1. Le siège de la matière

5. Les textes les plus importants au plan fédéral sont la *Loi fédérale sur la protection des données* du 19 juin 1992 (LPD, RS 235.1), entrée en vigueur le 1^{er} juillet 1993, et son ordonnance d'exécution du 14 juin 1993 (OLPD, RS 235.11), également entrée en vigueur le 1^{er} juillet 1993.

6. De façon caractéristique, la LPD constitue une *réglementation unique* en ce sens que son application ne dépend pas d'un support particulier ou d'une technique spécifique de récolte et de traitement des données (neutralité technologique) et qu'elle s'applique aussi bien aux personnes privées qu'à l'administration publique, aux personnes physiques et aux personnes morales, quel que soit le type de traitement visé[7].

7. L'art. 3 litt. a LPD précise qu'il faut entendre par données personnelles (données) "*toutes les informations qui se rapportent à une personne identifiée ou identifiable*". Des règles particulières s'appliquent aux données sensibles et aux profils de la personnalité, notions également définies par la loi[8]. La notion de traitement est large puisqu'elle inclut "*toute opération relative à des données personnelles - quels que soient les moyens et procédés utilisés - notamment la collecte, la conservation, l'exploitation, la modification, la communication, l'archivage ou la destruction de données*" (art. 3 litt. e LPD).

8. L'art. 2 al. 2 LPD réserve pourtant un certain nombre de situations particulières dans lesquelles la loi n'est pas applicable. C'est par exemple le cas pour des procédures judiciaires pendantes (litt. c) ou dans l'hypothèse de "*données personnelles qu'une personne physique traite pour un usage exclusivement personnel et qu'elle ne communique pas à des tiers*" (litt. a). Certains en déduisent vraisemblablement à tort l'inapplicabilité de la loi aux messages électroniques (*emails*) purement privés[9].

2. Les principes matériels du traitement des données dans la LPD

9. La LPD ne contient aucune interdiction de principe du traitement des données personnelles ; celui-ci doit simplement intervenir de manière licite, en respectant en particulier un certain nombre de principes matériels contenus dans la loi.

a. La licéité (art. 4 al. 1^{er} LPD)

10. Le principe de la licéité, qui s'attache avant tout à la collecte des données, prohibe de façon générale tout agissement déloyal, affirmations fallacieuses, tromperie, menaces ou dol[10]. Sont également visées les collectes de données dont l'illicéité résulterait d'infractions pénales sur la soustraction de données (art. 143 et art. 179^{novies} CP), la violation d'un secret professionnel (art. 321 et 321^{bis} CP) ou encore de fabrication (art. 162 CP) [11].

b. La bonne foi (art. 4 al. 2 LPD)

11. On a en particulier déduit du principe fondamental de la bonne foi l'interdiction, en règle générale, d'une collecte de données qui interviendrait contre la volonté, ou au moins à l'insu de la personne concernée[12]. On y rattache également des notions de transparence et de prévisibilité du traitement des données personnelles. Dans le domaine des nouvelles technologies et sans aller jusqu'à imposer, comme en droit européen, que la personne concernée soit préalablement informée de plusieurs aspects du traitement, ce principe commanderait toutefois, en conformité avec la recommandation du Conseil de l'Europe n° R(99)5 du 23 février 1999, que toute personne soit informée sur les risques inhérents au système, si le traitement des données intervient sur un réseau peu sûr[13].

c. La proportionnalité (art. 4 al. 2 LPD)

12. En vertu du principe de la proportionnalité, seules les données nécessaires à un but déterminé devraient être traitées. Son respect implique une pesée des intérêts entre le résultat recherché et le moyen utilisé[14].

13. Pour un auteur en tout cas, il serait même contraire au principe de la proportionnalité de collecter des données lorsque l'accès au service est gratuit, notamment pour la consultation d'un journal ou d'un site informatif et n'implique pas de dialogue avec l'utilisateur[15].

d. La finalité (art. 4 al. 3 LPD)

14. Selon l'art. 4 al. 3 LPD, "*les données personnelles ne doivent être traitées que dans le but qui est indiqué lors de leur collecte, qui est prévu par une loi ou qui ressort des circonstances*".

15. Le respect de ce principe implique la détermination préalable d'une finalité à la collecte des données et l'obligation d'utiliser ces données uniquement en fonction de cette finalité ou du moins de manière compatible[16]. Par conséquent, une collecte illimitée de données

pour des utilisations indéterminées de même que la création de banques de données à usages multiples non définis serait illicite.

e. L'exactitude des données (art. 5 LPD)

16. Ce principe a pour corollaire le droit de la personne concernée de requérir la rectification des données inexactes. Il implique également l'obligation de mise à jour des fichiers et doit être apprécié de façon relative en cas de jugement de valeur, dont le caractère litigieux pourra le cas échéant être mentionné (voir art. 15 al. 2 LPD).

f. La communication de données à l'étranger (art. 6 LPD)

17. La communication est définie largement à l'art. 3 litt. f LPD comme "le fait de rendre des données personnelles accessibles, par exemple en autorisant leur consultation, en les transmettant ou en les diffusant". L'art. 6 LPD pose comme principe l'interdiction de la communication des données personnelles à l'étranger "si la personnalité des personnes concernées devait s'en trouver gravement menacée, notamment du fait de l'absence d'une protection des données équivalente à celle qui est garantie en Suisse". Ce n'est pourtant pas le cas des pays membres de l'Union européenne, du fait de la l'adoption de la Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données^[17].

18. L'art. 6 al. 2 LPD prévoit encore la déclaration préalable obligatoire du fichier en cause s'il est prévu que des données soient transmises à l'étranger dans les cas où la communication ne découle pas d'une obligation légale ou a lieu à l'insu des personnes concernées^[18].

g. La sécurité (art. 7 LPD)

19. Selon l'art. 7 LPD, "*les données personnelles doivent être protégées contre tout traitement non autorisé par des mesures organisationnelles et techniques appropriées*". Il s'agit de garantir en particulier la confidentialité du traitement des données, leur disponibilité et leur intégrité. L'adéquation des mesures prises dépendra en particulier des finalités du traitement, de la nature des données traitées et de l'évolution technologique. Les mesures envisageables, détaillées aux art. 8 à 12 OLPD, visent notamment le personnel, le matériel, l'accès au locaux, le logiciel et l'organisation de l'entreprise.

20. À cet égard, l'art. 8 al. 1^{er} OLPD mentionne expressément les réseaux télématiques :

"La personne privée qui traite des données personnelles ou qui met à disposition un réseau télématique assure la confidentialité, la disponibilité et l'exactitude des données afin de garantir de manière appropriée la protection des données. Elle protège les systèmes notamment contre les risques de:

a. destruction accidentelle ou non autorisée;

b. perte accidentelle;

c. erreurs techniques;

d. falsification, vol ou utilisation illicite;

e. modification, copie, accès ou autre traitement non autorisés".

h. Le droit d'accès (art. 8 à 10 LPD)

21. Les art. 8 à 10 LPD traitent du droit d'accès, qui s'étend à toutes les données concernant le requérant contenues dans un fichier ainsi qu'au but et éventuellement à la base juridique du traitement et des catégories de données personnelles traitées, de participants au fichier et de destinataires des données. L'art. 8 al. 6 LPD précise que nul ne peut renoncer par avance à son droit d'accès, même si l'art. 9 LPD prévoit la possibilité de le restreindre, en particulier en cas d'intérêt public prépondérant ou d'intérêt prépondérant d'un tiers ou encore de risque de compromission d'une instruction pénale ou d'une autre procédure d'instruction. L'art. 10 al. 1^{er} LPD prévoit en outre une restriction en faveur d'un fichier utilisé exclusivement pour la publication dans la partie rédactionnelle d'un média à caractère périodique pour protéger les sources d'information ou un droit de regard sur les projets de publication ainsi que, de manière générale, la libre formation de l'opinion publique. Enfin, l'art. 10 al. 2 LPD ménage le droit aux journalistes de refuser ou restreindre la communication des renseignements demandés, voire d'en différer l'octroi, lorsqu'un fichier leur sert exclusivement d'instrument de travail personnel[19].

3. Le traitement des données par des personnes privées (art. 12 à 15 LPD)

22. En vertu de l'art. 12 al. 1^{er} LPD, "*quiconque traite des données personnelles ne doit pas porter une atteinte illicite à la personnalité des personnes concernées*". L'art. 13 al. 1^{er} LPD précise en outre qu'"*une atteinte à la personnalité est illicite à moins d'être justifiée par le consentement de la victime, par un intérêt prépondérant privé ou public, ou par la loi*".

23. Souvent, l'illicéité d'une atteinte à un droit de la personnalité dépendra en grande partie des circonstances du cas d'espèce. Pour faciliter l'application de la loi, l'art. 12 al. 2 LPD érige, sous une forme non exhaustive, une fiction d'atteinte illicite, notamment en cas de violation des principes définis aux art. 4 à 7 de la loi, lors d'un traitement des données contre la volonté expresse de la personne concernée ou encore en cas de communication à des tiers de données sensibles ou de profils de la personnalité.

24. Par ailleurs, l'art. 12 al. 3 LPD précise qu'en règle générale, "*il n'y a pas atteinte à la personnalité lorsque la personne concernée a rendu les données accessibles à tout un chacun et ne s'est pas opposée formellement au traitement*". On ne pourrait cependant déduire d'une participation à un forum de discussions ou de l'envoi des tels messages électroniques sur des listes de discussions, sans autres éléments, que ces conditions sont satisfaites. Un consentement explicite de la personne concernée est nécessaire[20].

25. L'art. 13 LPD réserve l'existence de motifs justificatifs, qui rendent licites une atteinte qui aurait pu être illicite. En vertu de l'art. 13 al. 1^{er} LPD, ces motifs justificatifs sont le consentement de la victime, un intérêt prépondérant privé ou public ou la loi. Par ailleurs, l'art. 13 al. 2 LPD contient une liste non exhaustive des situations dans lesquelles les intérêts prépondérants de la personne qui traite les données personnelles pourraient être pris en compte[21]. Contrairement à l'art. 12 al. 2 LPD, il ne s'agit toutefois pas d'une fiction et le juge conserve un large pouvoir d'appréciation[22].

26. Le consentement de la personne concernée, comme en droit de la personnalité classique, doit être libre, spécifique, éclairé et précis[23], ce qui dépendra avant tout de la qualité de l'information préalable qui lui aura été fournie. Il doit évidemment porter sur le traitement qui sera réellement effectué et ne peut être général, illimité ou irrévocable[24]. Le cas échéant, le droit d'accès permettra de le contrôler.

27. La loi ne soumet cependant le consentement à aucune forme particulière, pour autant qu'il soit dénué d'ambiguïté. C'est dire en particulier qu'il peut résulter de l'envoi d'une communication électronique spécifique ou de l'adhésion à des conditions générales en ligne, par exemple par l'appui sur une touche[25].

28. Quant aux autres motifs justificatifs, la détermination de l'intérêt privé ou public prépondérant suppose une pesée des intérêts qui prenne en compte la nature des données et la finalité du traitement. Pour la loi, il s'agira le plus souvent d'une réglementation de droit public[26].

29. L'art. 14 LPD autorise le traitement des données par un tiers, qui pourra s'appuyer sur les mêmes motifs justificatifs que son mandant et pour autant que le traitement ne soit pas modifié ou étendu, ce qu'il appartiendra au mandant de vérifier[27]. La délégation de traitement est en outre subordonnée à l'absence d'obligation légale ou contractuelle de garder le secret.

30. L'art. 15 LPD aborde les questions procédurales, en se référant principalement aux règles générales de la protection de la personnalité contenues aux art. 28 *et seq.* du Code civil du 10 décembre 1907 ("CC", RS 210), tout en apportant quelques nuances[28]. Il suffit ici de préciser que le demandeur devra apporter la preuve d'une atteinte illicite à sa personnalité, même si sa tâche est facilitée par la fiction de l'art. 12 al. 2 LPD.

4. Le traitement des données par des organes fédéraux (art. 16 à 25 LPD)

31. Par rapport aux règles énoncées ci-dessus en ce qui concerne le traitement par des personnes privées, applicables également lorsque les organes fédéraux exercent des activités de droit privé (art. 23 LPD), le traitement des données personnelles par des autorités fédérales se caractérise par la nécessité d'une base légale (art. 17 LPD). En cas de traitement de données sensibles ou de profils de la personnalité, cette base légale sera en principe une loi fédérale[29]. Alternativement, le traitement est autorisé si la personne concernée y a consenti ou a rendu les données en cause accessibles à tout un chacun (art. 17 al. 2 LPD).

32. En revanche, la communication, sur demande, du nom, du prénom, de l'adresse et de la date de naissance d'une personne n'est pas soumise à l'exigence d'une base légale, si, parmi d'autres situations envisagées par l'art. 19 LPD :

"a. le destinataire a, en l'espèce, absolument besoin de ces données pour accomplir sa tâche légale;

b. la personne concernée y a, en l'espèce, consenti ou les circonstances permettent de présumer un tel consentement;

c. la personne concernée a rendu ces données accessibles à tout un chacun ou si

d. le destinataire rend vraisemblable que la personne concernée ne refuse son accord ou ne s'oppose à la communication que dans le but de l'empêcher de se prévaloir de prétentions juridiques ou de faire valoir d'autres intérêts légitimes; dans la mesure du possible, la personne concernée sera auparavant invitée à se prononcer".

33. L'art. 20 LPD confère encore à la personne concernée qui rend vraisemblable un intérêt légitime le droit de s'opposer à la communication de données personnelles.

34. De façon générale, les données personnelles devenues inutiles doivent être rendues anonymes ou détruites, à moins d'obligation de conservation au titre de preuve ou par mesure de sûreté ou encore de dépôt aux archives fédérales (art. 21 LPD). Enfin, des conditions plus souples sont instaurées pour des traitements anonymes à des fins de recherche, de planification et de statistiques (art. 22 LPD).

35. Les voies de droit usuelles en cessation ou en constatation d'un traitement illicite ainsi que les possibilités de rectification de destruction ou de publication sont ouvertes à "quiconque a un intérêt légitime" (art. 25 LPD).

5. Le préposé fédéral à la protection des données (art. 26 à 32 LPD)

36. Les art. 26 à 32 LPD concernent la nomination, le statut et le rôle du préposé fédéral à la protection des données.

37. En vertu de l'art. 27 LPD, qui lui confère par ailleurs un certain pouvoir investigateur, "le préposé surveille l'application par les organes fédéraux de la présente loi et des autres dispositions fédérales relatives à la protection des données". En cas de violation, il peut émettre une recommandation qui pourra être transmise à l'organe fédéral concerné. Dans le secteur privé, le préposé a également le pouvoir d'établir les faits d'office et d'édicter des recommandations, qui pourront le cas échéant être portées devant la commission fédérale de la protection des données pour décision (art. 29 LPD).

6. Sanctions pénales (art. 34 et 35 LPD)

38. La violation des obligations de renseigner, de déclarer et de collaborer par les personnes privées sera, sur plainte, punie des arrêts ou de l'amende (art. 34 et 35 LPD).

7. Secret des télécommunications

39. Dans un arrêt du 5 avril 2000, le Tribunal fédéral a considéré que la messagerie électronique était couverte par le secret des télécommunications^[30]. Il s'agit donc d'en étudier brièvement les contours.

40. En vertu de l'art. 321^{ter} CP (violation du secret des postes et des télécommunications),

"¹ Celui qui, en sa qualité de fonctionnaire, d'employé ou d'auxiliaire d'une organisation fournissant des services postaux ou de télécommunication, aura transmis à un tiers des renseignements sur les relations postales, le trafic des paiements ou les télécommunications de la clientèle, ouvert un envoi fermé ou cherché à prendre connaissance de son contenu ou encore fourni à un tiers l'occasion de se livrer à un tel acte sera puni de l'emprisonnement ou de l'amende.

² De même, celui qui aura déterminé par la tromperie une personne astreinte au secret en vertu du 1^{er} alinéa à violer ce secret sera puni de l'emprisonnement ou de l'amende.

³ La violation du secret postal ou du secret des télécommunications demeure punissable après que l'emploi ou la charge ont pris fin.

⁴ La violation du secret postal ou du secret des télécommunications n'est pas punissable en tant qu'elle est requise pour déterminer l'ayant droit ou pour prévenir la survenance de dommages.

⁵ L'article 179^{octies} ainsi que les dispositions des législations fédérale et cantonales statuant une obligation de renseigner une autorité ou de témoigner en justice sont réservés".

41. L'article 179^{octies} CP vise les mesures officielles de surveillance ordonnée par un juge "aux fins de poursuivre ou de prévenir un crime ou un délit dont la gravité ou la particularité justifie l'intervention".

42. Enfin, l'art. 43 de la *Loi fédérale sur les télécommunications* du 30 avril 1997 ("LTC", RS 784.10) contient également une obligation de maintien du secret : "Il est interdit à toute personne qui a été ou qui est chargée d'assurer un service de télécommunication de donner à des tiers des renseignements sur les communications des usagers; de même, il lui est interdit de donner à quiconque la possibilité de communiquer de tels renseignements à des tiers". L'art. 44 LTC, complété par les art. 6 à 11 de l'*Ordonnance du Conseil fédéral sur le service de surveillance de la correspondance postale et des télécommunications* du 1^{er} décembre 1997 (RS 780.11), met en place la procédure et détaille les conditions auxquelles une surveillance peut intervenir. En bref, un service spécial, rattaché au Département fédéral de l'environnement, des transports, de l'énergie et de la communication, est chargé de la coordination (parfois de l'exécution) des mesures de

surveillance et de l'acheminement des requêtes de surveillance aux fournisseurs de services de télécommunications, qui ont droit à un dédommagement et ne peuvent en aucun cas agir de leur propre chef.

Conclusion

43. La réglementation suisse sur la protection des données personnelles sur Internet est similaire à bien des égards à celle de la Directive communautaire en la matière. Elle offre certainement une protection adéquate, qui s'inscrit également dans la ligne des recommandations récentes du Conseil de l'Europe.

44. Cependant, la mise en oeuvre concrète des mécanismes de protection prévus par la *Loi fédérale sur la protection des données* dépend essentiellement des utilisateurs du Réseau eux-mêmes, dans la mesure où il serait illusoire aujourd'hui d'escompter que l'ensemble des fournisseurs de contenu, de services, d'hébergement et d'accès sur Internet implémentent spontanément des politiques de traitement de données personnelles satisfaisant à tous les égards aux exigences légales.

45. Dans ce cadre, qui nécessite une coordination internationale importante, aucune réglementation spécifique nouvelle n'est prévue en droit suisse ; en revanche, le gouvernement helvétique est activement impliqué dans les efforts internationaux, menés notamment au sein du Conseil de l'Europe. Par ailleurs, le *Préposé fédéral à la protection des données* a déjà édicté un certain nombre de recommandations, tant à l'usage des utilisateurs que des fournisseurs de service sur Internet, prônant la transparence et l'information préalable.

Bibliographie

> Laurent Baeriswyl et Grégoire Mangeat, "Protection des données personnelles sur Internet : la situation en Suisse", *Juriscom.net*, Chroniques francophones, 21 juin 2000, <<http://www.juriscom.net/chr/2/ch20000621.htm>> ;

> Jérôme Bénédicte, *Internet et le respect du secret professionnel de l'avocat*, in *L'avocat moderne*, Regards sur une profession dans un monde qui change, Mélanges publiés par l'Ordre des Avocats Vaudois à l'occasion de son Centenaire, Bâle 1998, p. 267 ss ;

> Barbara M. Nestlé, *Die Übernahme allgemeiner Geschäftsbedingungen bei Internetangeboten (nach schweizerischem, europäischem und amerikanischem Konsumentenschutzrecht)*, in *Geschäftsplattform Internet - Rechtliche und praktische Aspekte*, Zurich, ZIK Band 10, 2000.

> Gérald Page, *Autoroutes de l'information et protection des données*, in *Information Highway*, Beiträge zu rechtlichen und tatsächlichen Fragen, édité par Reto M. Hilty, Berne 1996, p. 353-393 ; *idem*, Fiches juridiques suisses n° 1404 à 1406, Genève 1993 et 1996 ;

- > Kosmas Tsiraktsopoulos et Frédéric Schoenbett, "La protection des données et Internet", *Flash Informatique (EPFL) - Spécial Sécurité*, Lausanne 2000, p. 16-19 ;
- > Fridolin M. R. Walther, "Das Anwaltsgeheimnis im E-mail-Zeitalter eine Problemskizze", *RSJ* 96 (2000), p. 357-366 ;
- > Jean-Philippe Walter, "La protection des données dans le cyberspace", *Medialex* 2/00, p. 88-96 ;
- > Ursula Widmer et Konrad Bähler, *Rechtsfragen beim Electronic Commerce Sichere Geschäftstransaktionen im Internet*, 2^{ème} éd., Zurich, Orell Füssli, 2000, p. 239-280.

Notes

(*) Docteur en droit, LL.M. (Columbia), Chargé de cours aux Universités de Fribourg et de Neuchâtel, admis au barreau de New York, avocat, Genève. Email : jaccard@ttv.ch.

[1] Art. 28 du Code civil suisse du 10 décembre 1907 ("CC", RS 210). Voir Gérald Page, *Autoroutes de l'information et protection des données*, Bern, Information Highway, 1996, p. 386-390.

[2] Art. 47 de la *Loi fédérale sur les banques et les caisses d'épargne* du 8 novembre 1934 ("LB", RS 952.0).

[3] Art. 320 à 321^{bis} du Code pénal du 21 décembre 1937 ("CP", RS 311.0). Voir Jérôme Bénédicte, *Internet et le respect du secret professionnel de l'avocat*, in *L'avocat moderne, Regards sur une profession dans un monde qui change*, Mélanges publiés par l'Ordre des Avocats Vaudois à l'occasion de son Centenaire, Bâle, 1998, p. 267 ss ; Fridolin M. R. Walther, "Das Anwaltsgeheimnis im E-mail-Zeitalter eine Problemskizze", *RSJ* 96 (2000), p. 357 ss.

[4] Voir encore récemment un arrêt de la Cour européenne des droits de l'homme du 16 février 2000, dans la cause *Amann c. Suisse*, où il est rappelé que la notion de vie privée ne doit pas être interprétée de façon restrictive et n'exclut pas les activités professionnelles ou commerciales (§65).

[5] Le texte est disponible à l'adresse <http://www.coe.fr/dataprotection/Treaties/Convention%20108%20F.htm>.

[6] Le texte est disponible à l'adresse <http://www.coe.fr/dataprotection/rec/flignes.htm>.

[7] Gérald Page, *Autoroutes de l'information...*, *op. cit.*, note 1, p. 353.

[8] "Art. 3 Définitions

On entend par [...]

c. données sensibles, les données personnelles sur:

1. les opinions ou activités religieuses, philosophiques, politiques ou syndicales,

2. la santé, la sphère intime ou l'appartenance à une race,

3. des mesures d'aide sociale,

4. des poursuites ou sanctions pénales et administratives;

d. profil de la personnalité, un assemblage de données qui permet d'apprécier les caractéristiques essentielles de la personnalité d'une personne physique".

[9] Ursula Widmer et Konrad Bähler, *Rechtsfragen beim Electronic Commerce Sichere Geschäftstransaktionen im Internet*, 2^{ème} éd., Zurich, Orell Füssli, 2000, p. 247-248. *Contra* : Gérald Page, *Autoroutes de l'information...*, *op. cit.*, note 1, p. 362.

[10] Jean-Philippe Walter, "La protection des données dans le cyberspace", *Medialex* 2/00, p. 90.

[11] Gérald Page, Fiche juridique suisse n° 1404, p. 10.

[12] Jean-Philippe Walter, *loc. cit.*, note 10, p. 90.

[13] Jean-Philippe Walter, *loc. cit.*, note 10, p. 90-91.

[14] Laurent Baeriswyl et Grégoire Mangeat, "Protection des données personnelles sur Internet : la situation en Suisse", *Juriscom.net*, Chroniques francophones, 21 juin 2000, §7, <<http://www.juriscom.net/chr/2/ch20000621.htm>>.

[15] Jean-Philippe Walter, *loc. cit.*, note 10, p. 91.

[16] Jean-Philippe Walter, *loc. cit.*, note 10, p. 91.

[17] Journal officiel n° L 281 du 23 novembre 1995, p. 31 à 50. Il semblerait d'ailleurs qu'en application de l'art. 25 paragraphe 6 de la Directive 95/46/EC, la Commission européenne s'apprête à considérer que le niveau de protection des données en Suisse était adéquat au regard de la Directive (voir l'Avis 5/99 du 7 juin 1999 du Groupe de travail concernant le niveau de protection des données à caractère personnel en Suisse).

[18] Kosmas Tsiraktsopoulos et Frédéric Schoenbett, "La protection des données et Internet", *Flash Informatique (EPFL) - Spécial Sécurité*, Lausanne 2000, p. 17.

[19] Voir de manière générale Gérald Page, *Autoroutes de l'information...*, *op. cit.*, note 1, p. 386-390.

[20] Jean-Philippe Walter, *loc. cit.*, note 10, p. 92 ; Gérald Page, *Autoroutes de l'information...*, *op. cit.*, p. 367.

[21] "Art. 13 Motifs justificatifs

[...]

² *Les intérêts prépondérants de la personne qui traite des données personnelles entrent notamment en considération si:*

a. le traitement est en relation directe avec la conclusion ou l'exécution d'un contrat et les données traitées concernent le cocontractant;

b. le traitement s'inscrit dans un rapport de concurrence économique actuel ou futur avec une autre personne, à condition toutefois qu'aucune donnée personnelle traitée ne soit communiquée à des tiers;

c. les données personnelles sont traitées dans le but d'évaluer le crédit d'une autre personne, à condition toutefois qu'elles ne soient ni sensibles ni constitutives de profils de la personnalité et qu'elles ne soient communiquées à des tiers que si ceux-ci en ont besoin pour conclure ou exécuter un contrat avec la personne concernée;

d. les données personnelles sont traitées de manière professionnelle exclusivement en vue d'une publication dans la partie rédactionnelle d'un média à caractère périodique;

e. les données personnelles sont traitées à des fins ne se rapportant pas à des personnes, notamment dans le cadre de la recherche, de la planification ou de la statistique, à condition toutefois que les résultats soient publiés sous une forme ne permettant pas d'identifier les personnes concernées;

f. Les données recueillies concernent une personnalité publique, dans la mesure où ces données se réfèrent à son activité publique".

[22] Gérald Page, *loc. cit.*, note 11, p. 6.

[23] Gérald Page, *loc. cit.*, note 11, p. 6.

[24] Jean-Philippe Walter, *loc. cit.*, note 10, p. 93.

[25] voir par exemple, Barbara M. Nestlé, *Die Übernahme allgemeiner Geschäftsbedingungen bei Internetangeboten (nach schweizerischem, europäischem und amerikanischem Konsumentenschutzrecht)*, in *Geschäftsplattform Internet - Rechtliche und praktische Aspekte*, Zurich, ZIK Band 10, 2000, p. 264.

[26] Gérald Page, *loc. cit.*, note 11, p. 7.

[27] Gérald Page, *loc. cit.*, note 11, p. 12.

[28] Pour un développement complet de ces questions, voir Gérald Page, *loc. cit.*, note 11, p. 13 ss.

[29] Voir en particulier la *Loi fédérale sur la création et l'adaptation de bases légales concernant le traitement de données personnelles* du 24 mars 2000 (RS 141.0), entrée en vigueur le 1^{er} septembre 2000, qui procède aux adaptations nécessaires pour un certain nombre d'actes législatifs fédéraux.

[30] ATF 126 I 50 ("Swissonline").