

Article publié : ne faire référence qu'à la version publiée

DE HERT P., DE VRIES K. & GUTWIRTH S., "La limitation des 'perquisitions en ligne' par un renouvellement des droit fondamentaux", Note d'observations sur Cour constitutionnelle fédérale allemande, 27 février 2008 (*Online Dursuchung*), *Revue du droit des Technologies de l'Information*, Jurisprudence, 2009, 89-92¹

L'arrêt du 27 février 2008 de la Cour constitutionnelle fédérale allemande sur les perquisitions secrètes "en ligne" par des agences gouvernementales est un arrêt jalon, parce qu'il constitue un nouveau "droit fondamental à la protection de la confidentialité et l'intégrité des systèmes d'information technologiques" à partir de l'interprétation de la Constitution allemande. L'arrêt s'ajoute à d'autres décisions cruciales relatives à la protection de la vie privée dans lesquelles la Cour avait déjà élaboré "le droit à l'autodétermination informationnelle" (1983) et le droit à la "protection absolue du noyau dur de la vie privée" (2004).

The Federal German Constitutional Court published on 27 February 2008 a landmark ruling about the constitutionality of secret online searches of computers by government agencies. The decision constitutes a new "basic right to the confidentiality and integrity of information-technological systems" as derived from the German Constitution. The decision complements earlier landmark privacy rulings by the Constitutional Court that had introduced the "right to informational self-determination" (1983) and the right to the "absolute protection of the core area of the private conduct of life"(2004).

Le *spyware* secrètement installé est un instrument fort apprécié par les internautes et criminels intéressés par les données à caractère personnel. Ce logiciel permet en effet de surveiller chaque opération d'un utilisateur d'ordinateur en temps réel ou même de lire un disque dur à distance. Evidemment, cette dernière possibilité a également suscité l'intérêt de nombre de services policiers. En 2008 une véritable lutte politique et juridique a été menée en Allemagne² autour du droit qu'aurait la police dans certains cas d' « implanter » ce genre de *spyware* dans les ordinateurs de suspects afin d'en rendre possible la *Online-Durchsuchung*³.

D'après l'arrêt du 27 février 2008⁴, une telle « perquisition en ligne » implique qu'« un accès secret à un système de technique d'information par infiltration technique⁵ » est créé « par lequel l'usage du système peut être observé et ses moyens de mémorisation déchiffrés et

¹ Les auteurs font partie du centre de recherches *Law, Science, Technology & Society* à la Vrije Universiteit Brussel : www.vub.ac.be/LSTS

² Cf. «Call for worldwide protests against surveillance », *EDRI-gram, Biweekly newsletter about digital civil rights in Europe*, nr.6.16, 27 août 2008, et "German Protests in over 30 cities against surveillance On 31 May 2008, privacy activists organized new rallies in more than 30 cities across Germany", *EDRI-gram. Biweekly newsletter about digital civil rights in Europe*, nr.6.13, 2 juillet 2008.

³ Au sujet de l'histoire de cette terminologie ambiguë voir : T. Böckenförde, « Auf dem Weg zur elektronischen Privatsphäre », *Juristischezeitung (JZ)* 2008, 929. Nous avons opté pour la traduction littérale de « Dursuchung » par « fouille », après avoir hésité au sujet d' « écoute » et « investigation », la raison étant que « fouille » a une dimension active (contrairement à « écoute ») et que le terme se rapproche plus littéralement à « Dursuchung » (qu'« investigation »)

⁴ *Online Durchsuchung*, Bundesverfassungsgerichtshof 27 février 2008, 1 BvR 370/07, 1 BvR 595/07

⁵ « ...heimlicher Zugriff auf informationstechnische Systeme mittels technischer Infiltration » (paragraphe 7, *Online Durchsuchung*, Bundesverfassungsgerichtshof 27 février 2008).

lus »⁶. Les documents officiels parlent prudemment de « Remote Forensic Software »⁷, mais plus trivialement les programmes installés secrètement sont mieux connus sous le nom de *Polizeitrojanner* ou – lorsqu’il s’agit de l’usage au niveau fédéral par la *Bundeskriminalamt* – de soi-disant *Bundestroyaner*.

Par son arrêt du 27 février 2008, la Cour constitutionnelle fédérale allemande, la *Bundesverfassungsgericht*, a jugé qu’une loi amendée⁸ en décembre 2006 en Rhénanie-du-Nord-Westphalie qui accordait de larges compétences en matière de perquisitions en ligne aux services de renseignements de cet état fédéré, était inconstitutionnelle. Deux questions étaient centrales dans le jugement de la *Bundesverfassungsgericht*. D’abord il fallait vérifier quel droit fondamental était éventuellement affecté par la loi et ensuite si ces atteintes restaient ou non dans les limites constitutionnelles admissibles.

La réponse de la Cour à la première question est surprenante. Après avoir exposé amplement pourquoi la loi sur les perquisitions en ligne ne porte pas atteinte aux droits fondamentaux existants comme le *droit au secret des télécommunications* (art.10 GG), le *droit au domicile* (art.13 GG) ou un des droits dérivés du droit général de la personnalité (*Algemeinen Persönlichkeitsrecht* art.1 premier alinéa et art. 2 premier alinéa, GG) tel que le *droit de la protection de la vie privée* (BVG 15 janvier 1970, BverfGE 27, 344) ou le *droit à l’autodétermination informationnelle* (BVG 15 décembre 1983, BVGE 65, 1), la Cour crée sur la base du droit général de la personnalité un tout nouveau droit fondamental à la protection de « la confidentialité et l’intégrité des systèmes d’information technologiques ». Ce nouveau droit fondamental en matière de technologie de l’information doit compléter les droits fondamentaux existants là où ils font défaut.

Ainsi, la Cour a jugé que le *droit au secret des télécommunications* (art. 10 GG) offre une protection insuffisante contre la perquisition en ligne parce qu’il protège, certes, la communication même mais point les données sauvegardées (§ 185-190). L’*inviolabilité du domicile* (art. 13 GG) semble également difficile à invoquer contre les perquisitions en ligne parce que pour la police il est indifférent qu’un ordinateur soit utilisé chez soi ou dans un lieu public. En effet, la question de savoir si un ordinateur se trouve chez soi ou non devient le cas échéant un détail plus ou moins aléatoire : le mur d’une maison ne représente pas une difficulté supplémentaire qui doit être contournée technologiquement. La Cour rejette résolument (§ 191-195) l’idée d’une extension constitutionnelle de la protection du domicile, par laquelle on pourrait considérer un ordinateur portable, PDA ou téléphone mobile dans un lieu public comme une extension mobile et virtuelle du domicile : un *firewall* n’est pas un mur d’habitation⁹. Finalement la Cour pose que les *Ausprägungen* (expressions ou manifestations) formulées du droit général de la personnalité en 1970 (BVG 15 janvier 1970, BverfGE 27, 344, *Ehescheidungsakten*) et en 1983 (BVG 15 décembre 1983, BVGE 65,1, *Volkzählungsurteil*) n’offrent en la matière pas de protection efficace. Ainsi, le droit de 1970 ne tient compte que de la protection de la vie privée, alors que chaque système informatique personnel comporte probablement plus que des données purement privées (§ 197), et que le droit à l’autodétermination en matière d’information de l’arrêt de 1983 n’offre aucune solution

⁶ « heimliche Infiltration eines informationstechnischen Systems, mittels derer die Nutzung des Systems überwacht und seine Speichermedien ausgelesen werden können » (Leitsatz 2, *Online Durchsuchung*, Bundesverfassungsgerichtshof 27 février 2008).

⁷ <http://netzpolitik.org/2007/bka-proudly-presents-remote-forensic-software/>

⁸ Amendement du §5 Abs.2 No.11 du *Verfassungsschutzgesetz Nordrhein-Westfalen* (VSG-NRW), 20 décembre 2006, GVBl, NW 2006, 620.

⁹ Cf. Thomas Böckenförde, « Auf dem Weg zur elektronischen Privatsphäre », *Juristische Zeitung* (JZ) 2008, 926.

satisfaisante car une fouille en ligne n'aboutit généralement pas seulement à la collecte, l'enregistrement, la diffusion ou le traitement mais aussi à la lecture de grandes quantités de données déjà organisées (§198-200).

La deuxième question que la Cour devait examiner était dans quelle mesure les infractions au nouveau droit fondamentales autorisées par la loi de la Rhénanie du Nord-Westphalie sont en accord avec des restrictions constitutionnellement admissibles. En effet, tout comme la plupart des autres droits fondamentaux, le nouveau droit à « la confidentialité et à l'intégrité des systèmes technologiques informationnels » n'est pas un droit absolu.

D'après la Cour, la loi de la Rhénanie du Nord-Westphalie va trop loin parce qu'elle circonscrit les circonstances dans lesquelles la perquisition en ligne est possible par un renvoi beaucoup trop vague à l'art. 10 GG au sujet du secret des télécommunications. Un tel mode opératoire n'offre en effet pas de garantie pour l'inviolabilité de la *Kernbereich* ou du « noyau dur » de la vie privée en ce qu'il ne limite pas la perquisition en ligne à des circonstances exceptionnelles. Bien que la Cour juge que des buts préventifs ou des besoins de l'enquête dans le cadre des poursuites pénales peuvent très bien justifier certaines infractions concernant le nouveau droit à l'intégrité des systèmes informatiques (§ 207), celles-ci ne peuvent être qu'autorisées dans des conditions exceptionnelles et nommément, uniquement (a) après autorisation par un juge (§257 et 269) ou par une « instance indépendante et neutre » équivalente (§ 258 et § 260) ; (b) avec suffisamment de garanties qui assurent la protection absolue du noyau dur de la vie privée (§ 273 et 277) ; et (c) s'il y a des « indications effectives d'un danger concret » pour la vie, le bien-être corporel et la liberté des personnes, ou pour les fondements de l'Etat (§ 247).

Si ces conditions sévères sont remplies, des perquisitions en ligne peuvent avoir lieu, mais seulement si des mesures efficaces ont été mises en place pour que le noyau dur de la vie privée, qui comprend par exemple les sentiments et les relations intimes, soit protégé. Cette protection doit comporter des mesures techniques qui ont pour but d'éviter la collecte de données au sujet de ce *Kernbereich* de la vie privée. La Cour poursuit : « S'il y a des indications concrètes que dans un cas spécifique une mesure déterminée de la collecte de données enfreint le noyau dur de la vie privée, alors cette collecte ne peut en principe pas être appliquée » (§ 281). Si accidentellement des données de ce noyau sont quand même collectées, elles doivent immédiatement être effacées et ne peuvent sous aucune condition être transférées ou utilisées.

Quelle est maintenant la signification de la nouvelle loi fondamentale ? Les considérations les plus évidentes concernent naturellement la question de savoir comment ce nouveau droit fondamental à la « confidentialité et intégrité des systèmes d'information technologiques » va devenir opératoire dans le droit pénal¹⁰. Il y a encore beaucoup d'imprécisions concernant la portée et la signification exacte de ce droit fondamental¹¹. Il y a lieu de surcroît de se demander comment ce nouveau droit va se rapporter aux droits plus classiques comme l'inviolabilité du domicile (art. 13 GG), le droit au secret des communications électroniques (art.10 GG) ou le droit à l'« autodétermination informationnelle »¹². Qu'il y ait encore

¹⁰ Voir p.e. G. Hornung, « Ein neues Grundrecht », *Computer und Recht* 2008, 305-306.

¹¹ T.Hoeren, « Was ist das Grundrecht auf Integrität und Vertraulichkeit informationstechnischer Systeme? », *Multimedia und Recht* 2008, 365-366.

¹² Voir pour chevauchement éventuel du nouveau droit à la confidentialité et l'intégrité des systèmes informatiques d'une part, et les droits au domicile et au secret des télécommunications d'autre part, voir W. Hoffmann-Riem, « Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme », *Juristen Zeitung*, vol. 63, nr. 21, novembre 2008, 1021-1022.

beaucoup d'imprécisions n'empêche cependant pas que, d'une manière générale, il est admis que ce nouveau droit représente un seuil juridique dans le domaine des technologies de l'information et de la communication, et qu'il formera un complément précieux aux droits fondamentaux existants. Bien que le droit fondamental soit 'né' à l'intérieur du contexte du droit pénal, il pourrait, suite au principe de l'effet reflexe (« *Drittwirkung* »), avoir des effets horizontaux dans le domaine du droit à la protection des données personnelles, du droit de la concurrence, du droit de la consommation et du droit civil¹³. Ce qui est valable pour les *Polizeitrojaner*, *Bundestrojaner* ou toute autre forme *spyware* « implanté » par des autorités, ne manquera pas d'avoir également un impact sur le *spyware* à buts commerciaux ou personnels.

Plus fondamentalement, on peut se demander si ce nouveau droit mènera à ce que, à côté de la personnalité naturelle et juridique, on en arrivera à reconnaître une personnalité « digitale »¹⁴ et si, en marge de la sphère privée normale, une « sphère privée électronique »¹⁵ trouvera également sa protection.

¹³ Voir plus extensivement : A. Rosnagel & Schnabel, « Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und sein Einfluss auf das Privatrecht », *Neue Juristische Wochenschrift* 2008, forthcoming.

¹⁴ W. Schulz, « Protecting the digital personhood. German constitutional Law ». Présentation à la *ItechLaw2008 European Conference*, Barcelona, 7 novembre 2008.

¹⁵ T. Böckenförde, « Auf dem Weg zur elektronischen Privatsphäre », *Juristische Zeitung (JZ)* 2008, 939. A ce sujet voir aussi Paul De Hert et Serge Gutwirth, « Making sense of privacy and data protection. A prospective overview in the light of the future of identity, location based services and the virtual residence », IPTS, *Security and Privacy for the Citizen in the Post-September 11 Digital Age. A prospective overview*. 2003, IPTS-Technical Report Series, EUR 20823 EN <<ftp://ftp.jrc.es/pub/EURdoc/eur20823en.pdf>>, p. 158 et seq.