



HAL
open science

Droit et usages des nouvelles technologies : les enjeux d'une réglementation de la vidéosurveillance.

Eric Heilmann, Frédéric Ocqueteau

► To cite this version:

Eric Heilmann, Frédéric Ocqueteau. Droit et usages des nouvelles technologies : les enjeux d'une réglementation de la vidéosurveillance.. Droit et Société, Librairie générale de droit et de jurisprudence : Lextenso éditions/L.G.D.J., 1997. sic_00125571

HAL Id: sic_00125571

https://archivesic.ccsd.cnrs.fr/sic_00125571

Submitted on 21 Jan 2007

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Droit et usages des nouvelles technologies : les enjeux d'une réglementation de la vidéosurveillance

Droit et Société 36/37-1997
(p. 331-344)

Frédéric Ocqueteau *, Éric Heilmann **

Résumé

Les techniques de l'information et de la communication conditionnent de plus en plus fortement les relations sociales. C'est un champ de recherche en plein essor dont on peut enrichir la compréhension en montrant comment les réglementations extérieures à ces techniques les affectent à leur tour. L'objectif de cet article est double : d'une part, retracer le contexte au sein duquel s'inscrit l'actuelle opération de légalisation et de contrôle des technologies de vidéosurveillance par les préfets, c'est-à-dire dégager les présupposés politiques de la loi et observer les diverses simplifications du problème dans les textes d'application nécessaires à la mise en œuvre concrète ; d'autre part, confronter ces présupposés aux utilisations réelles (déclarées ou latentes) de la vidéosurveillance, à l'aide d'exemples tirés de diverses observations de terrain. Il ressort de cette confrontation que les « organisations » équipées sont de plus en plus poussées à afficher la carte d'un usage sécuritaire de la vidéosurveillance pour améliorer l'efficacité du travail policier contre l'insécurité urbaine, alors qu'il ne s'agit pas nécessairement de la vocation première de ces techniques.

Mise en œuvre et effectivité des normes - Sociologie réglementaire - Technologies de sécurité - Vidéosurveillance.

Summary

Law and Practice of New Technologies : Issues in Regulation of Close Circuit Television (CCTV)

Social relations are increasingly determined by information and communication techniques. A better understanding of this expanding field of research may be obtained by showing how regulations tend to alter the techniques themselves. The aim of this article is twofold : firstly, to describe the present context in which Prefects legalise and control CCTV techniques i.e. by revealing political assumptions underlying the law and observing the various simplifications of the problem within secondary norms necessary for its practical implementation ; secondly, to oppose

Les auteurs

Frédéric Ocqueteau

Sociologue et juriste. Chargé de recherche au CNRS, ses travaux portent sur les objets policiers, les ressources du marché et les nouvelles technologies de sécurité.

Son dernier ouvrage :

— *Les défis de la sécurité privée, protection et surveillance dans la France d'aujourd'hui*, Paris, l'Harmattan, 1997.

Éric Heilmann

Maître de conférences à l'Université Louis Pasteur de Strasbourg, est spécialisé dans les sciences de l'information et de la communication.

A notamment publié :

— *Science ou justice ?* (sous la dir.), Paris, éd. Autrement, 1994 ;

— *Nouvelles technologies, nouvelles régulations ?* (en collaboration avec A. Vitalis), Paris, IHESI-PirVilles, 1996.

* CNRS-Groupe d'analyse des politiques publiques (GAPP), École normale supérieure, 61, avenue du Président Wilson, F-94235 Cachan cedex.

** Groupe d'enseignement et de recherche sur la science, Université Louis Pasteur (GERSULP), 7, rue de l'Université, F-67000 Strasbourg.

F. Ocqueteau, É. Heilmann
Droit et usages des nouvelles technologies : les enjeux d'une réglementation de la vidéosurveillance

1. Pour un récent dossier complet sur les NTIC, voir *Problèmes économiques* (Paris, La Documentation française), mars 1996, n° 2464-2465.
2. M. LINDEKENS, *L'offre des biens de sécurité en Belgique*, Bruxelles, Politeia-ASBL, 1992.
3. F. OCQUETEAU, *Les défis de la sécurité privée*, Paris, L'Harmattan, 1997.
4. A. MIDOL, « Le recours à la technologie dans la sécurité privée », *Les Cahiers de la sécurité intérieure*, n° 21, 1995, p. 43-52.
5. Sur ce concept de *technoprévention* ou de *technostructure de la prévention*, voir R. DEDECKER, *La sécurité privée dans l'Europe des Douze* (Bruxelles, Politeia-ASBL, 1991, p. 149), qui la définit comme suit : « gestion sur le plan décisionnel par des groupes de spécialistes, de la production de besoins définis, de problèmes créés et de solutions apportées en matière de sécurité ». Cet auteur n'étaye pas outre mesure son propos par une description anatomique de cette technostructure mêlant les hommes et les techniques de sécurité, dont il est néanmoins indifférent qu'ils appartiennent au monde privé ou public.
6. On notera au passage que cette partition semble s'être imposée sans difficulté au monde de la police du renseignement et de la police judiciaire. Par exemple, E. REBSCHER, « La police allemande développe l'utilisation des nouvelles technologies », *Les Cahiers de la sécurité intérieure*, n° 21, 1995, p. 35-42.

these assumptions and real practices (stated and latent) in CCTV, using examples drawn from field research. This latter approach suggests that organisations equipped with CCTV are increasingly led to emphasise security aspects in order to improve the professional ability of policemen regarding urban insecurity, although this is not necessarily the principal role of these techniques.

CCTV - Implementation and effectiveness of norms - Sociology of regulation - Technologies of security.

Parmi ce qu'il est convenu d'appeler les « nouvelles technologies de l'information et de la communication » (NTIC) ¹, leurs éventuelles utilisations à des fins de sécurité ne sont apparues problématiques que récemment. Au moment où l'on a pris conscience qu'elles pouvaient également menacer les libertés fondamentales et la vie privée des citoyens, des entreprises et des particuliers ont multiplié les dispositifs de sécurité et de confidentialité disponibles en sécurisant les accès, authentifiant les utilisateurs ou cryptant les données. Les NTIC sont devenues une composante essentielle d'un vaste univers de services spécialisés dans la production et la vente de « biens de sécurité » difficiles à inventorier tant ils sont divers et variés ². Mais les secteurs d'activité impliqués dans la conception, la fabrication et la distribution de ces produits électroniques ont connu un tel développement au cours des années 1990 qu'un besoin de clarification puis de normalisation s'est fait de plus en plus pressant chez les consultants en matière de « sécurité privée » reconvertis dans le marketing public de ces technologies ³.

À cette occasion, une distinction entre *technologies de sécurité par destination* et *technologies de sécurité par incidence* ⁴ est inventée, ayant pour effet opératoire d'ajuster les NTIC aux visées des professionnels de la technoprévention ⁵. Ce découpage, classant les objets technologiques en fonction de leur nature supposée, permet de faire admettre que les acteurs de la sécurité publique auraient une vocation naturelle, sinon exclusive, à s'annexer les premières : techniques de protection physique, de (télé)détection et de (télé)surveillance, de vidéosurveillance, d'exploitations d'informations servant à l'identification ⁶. Aux secondes, les *technologies de sécurité par incidence*, seraient concédés les usages les plus divers, qui n'auraient à voir que marginalement avec la protection des biens et des personnes. En réalité, leur potentiel reste mobilisable par la police à tout moment, dès que les nécessités de la « raison d'État » s'en font sentir : domotique, téléassistance et tous autres outils supposés faciliter la vie en société moderne (cartes à mémoire multiservice, radiotéléphones, portables, micro-informatique), localiser les biens (marqueurs électroniques embarqués) et

mémoriser des opérations (cartes bancaires, télépéage sur autoroute, etc.).

Reste que la nécessité de légaliser l'usage de certaines de ces technologies s'impose, car elles apparaissent trop problématiques dans la société. C'est qu'à leur sujet, entre les citoyens et les polices, s'affrontent des points de vue idéologiques opposés à propos des *modus operandi* pour obtenir un meilleur niveau de sécurité ou de liberté. Des citoyens, relayés par des autorités administratives indépendantes, se sentant menacés dans leur vie privée par l'intrusion de ces nouvelles techniques de contrôle, en contestent les utilisations abusives. En face, les porte-parole des polices invoquent un « déficit de sécurité » à l'égard de nouvelles menaces qui s'amplifieraient dans un monde où disparaissent les frontières de la souveraineté territorialisée⁷. Ils soulignent les effets professionnels bénéfiques de ces techniques qui procureraient gains de temps et de mobilité, et surtout progrès dans le rassemblement des preuves. Plus fondamentalement, les autorités publiques admettent mal que les utilisations privées des NTIC — on pense notamment à un outil de communication tel qu'Internet — soient laissées sans contrôle entre les mains des citoyens, en raison du fait qu'elles pourraient engendrer des excès menaçant la sécurité collective⁸. Tout se passe alors comme si les impératifs de sécurité devaient nécessairement précéder les nouveaux moyens de la liberté, comme si la nécessité d'attenter aux libertés en matière de communication et d'information se justifiait par le prétendu « déficit de sécurité » soutenu par les élites policières.

En fait, se réactualise aujourd'hui un vieux contentieux à teneur déterministe et manichéenne, comme le souligne également Philippe Breton à propos des « autoroutes de la communication »⁹. Et il est bien difficile de garder une position sereine. De nouveaux croisés s'engagent, qu'ils soient philosophes¹⁰, juristes¹¹, chercheurs aux approches macro-sociopolitiques¹² ou microsociologiques¹³; derrière des angles d'attaque très variés, tous ont déjà fait peu ou prou le choix de résister, pour promouvoir le camp de la liberté contre celui de la sécurité. Les observations des premiers d'entre eux notamment sont saturées d'idéologie : elles occultent le plus souvent la question des utilisations ou des usages réels des techniques de sécurité, faute d'en avoir véritablement sondé les appropriations sociales, ce qui aurait pourtant le mérite de déplacer certains enjeux et de faire avancer la réflexion au lieu de la réduire à un antagonisme sommaire.

Pour en sortir, un certain nombre de sociologues ont montré comment on devait essayer de rendre compte des innovations technologiques. Thierry Vedel, discutant des apports de l'école de Bruno Latour et des chercheurs du Centre de sociologie de l'innovation, a fort heureusement problématisé la question¹⁴. Il plaide en particulier pour une articulation de la compréhension des

7. D. BIGO, *Polices en réseaux, l'expérience européenne*, Paris, Presses de la FNSP, 1996.

8. Sur la guerre que livrent les Services secrets aux pratiques de cryptage sur ce réseau, cf.

J. GUISEL, *Guerres dans le cyberspace, services secrets et Internet*, Paris, La Découverte, 1995.

9. P. BRETON, « Quel avenir dessinent les "autoroutes de l'information" ? » dans *L'État du monde*, Paris, La Découverte, 1996, p. 198-200, cf. p. 198.

10. J.J. DELFOUR, « La vidéosurveillance et le pouvoir du voir », *Lignes*, n° 27, 1996.

11. A. DE LAJARTE, « Fonctions et fictions des "miradors électroniques" publics : la "vidéosurveillance" dans la loi du 21 janvier 1995 », *La Semaine Juridique*, n° 36, 4 septembre 1996, p. 317-324 ; E. DARRAS et D. DEHARBE, « La politique du regard. Remarques sur la légalisation de la vidéosurveillance », dans CURAPP, *La gouvernabilité*, Paris, PUF, 1996, p. 77-90.

12. G. MARX, « La société de sécurité maximale », *Déviance et Société*, vol. 12, n° 2, 1988, p. 147-166.

13. M. LIANOS, *La poésie de la peur, le sujet hyper-régulier*, Thèse de doctorat, Paris, Université Paris VII, 1996, ronéo.

14. T. VEDEL, « Sociologie des innovations technologiques et usagers : introduction à une socio-politique des usages », dans A. VITALIS (ed.), *Médias et nouvelles technologies*, Rennes, Apogée, 1994, p. 13-34.

logiques techniques et des logiques sociales avec celle des logiques d'offre et des logiques d'usage, autrement dit, pour une mesure des effets conditionnants de la technique sur les relations sociales. Ces conseils valent également, nous semble-t-il, lorsqu'on observe les processus de codification, de canalisation et de légalisation de certaines des techniques de sécurité que nous venons d'évoquer. Au delà des intérêts immédiats poursuivis par ceux qui attribuent à la puissance publique la fonction de contrôler leur emploi, il nous paraît nécessaire de comprendre comment les systèmes de valeurs et de représentations des acteurs concernés se projettent dans ces technologies, pour en estimer l'effectivité probable. Une connaissance préalable des usages apportera de la plus-value si elle permet d'analyser comment ils peuvent être affectés par l'introduction extérieure de dispositifs réglementaires dans leur fonctionnement et les modifier en retour.

C'est pourquoi nous nous proposons, au vu de l'opération de légalisation de la vidéosurveillance engagée par la loi du 21 janvier 1995 et du décret du 17 octobre 1996¹⁵, de confronter les objectifs ayant explicitement présidé à ce texte, aux usages présents et à venir de cette technique. On sait que l'article 10 de cette loi prétend réglementer les systèmes de vidéosurveillance installés dans les lieux ouverts au public pour protéger les libertés contre de possibles abus ou détournements par les personnes qui les mettent en œuvre. Il prévoit une autorisation préfectorale délivrée au vu d'un dossier visé par une commission départementale créée *ad hoc* quand les lieux filmés sont particulièrement exposés à des risques d'agression ou de vols. Nous observerons comment le législateur, en définissant les « lieux », les « opérateurs » et les « finalités » des installations techniques de vidéosurveillance a obéi à une logique gouvernée par une conviction forte, bien que ne s'affichant jamais comme telle : l'espoir de maximiser durablement l'efficacité de la police actuellement confrontée à de très médiocres performances dans ses missions de prévention de l'insécurité urbaine. Notre hypothèse est que, souffrant d'un dangereux discrédit d'inefficacité dans ce domaine, en dépit d'une politique publique du ministère de l'Intérieur affichant depuis une quinzaine d'années comme prioritaire le redéploiement sur le terrain d'une « police de proximité » sans en avoir les retombées escomptées, les polices publiques ont particulièrement besoin d'annexer les prouesses supposées de ces techniques à leurs intérêts professionnels bien compris¹⁶. L'État affirme son autorité symbolique en légalisant les techniques de surveillance à distance, se réservant le droit d'intervenir si les utilisations atteignent son domaine de souveraineté. Parallèlement, il laisse aux spécialistes des libertés publiques le soin de se préoccuper de la mise en place de garde-fous pour contrer le zèle des opérateurs concurrents (policiers municipaux, agents de sécurité privés), manipulant ces techniques pour préve-

15. Loi n° 95-13 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité, *Journal officiel*, 24 janvier 1995 ; complétée par le décret n° 96-926 du 17 octobre 1996 relatif à la vidéosurveillance pris pour l'application de l'article 10 de la loi du 21 janvier 1995, *Journal officiel*, 20 octobre 1996 ; et la circulaire aux préfets du 22 octobre 1996, *Journal officiel*, 7 décembre 1996, p. 17835-17840.

16. Nous avons déjà été amenés à faire un constat analogue à propos du décret du 26 novembre 1991 réglementant les activités de surveillance à distance (télé-surveillance) et de l'arrêté du 3 novembre 1995 fixant les taux de redevances des bénéficiaires d'un numéro de téléphone réservé dans les activités de surveillance à distance dans F. OCQUETEAU, *op. cit.*, 1997, p. 118-119.

nir des incidents sur des espaces où la gestion de l'ordre échappe *de facto* aux polices d'État.

I. Les lieux de la vidéosurveillance

La représentation géographique de l'espace en trois composantes (public, privé, privé ouvert au public) semble toujours une nécessité logique pour le législateur, le juge ou le policier, dès lors qu'il s'agit de codifier l'usage d'une technique qui prétend filmer ce qui se passe à distance en vue de prévenir un trouble éventuel sur l'un de ces espaces. C'est qu'historiquement, les lieux à « policer » sont définis par la nature réactive ou proactive des pouvoirs de la police¹⁷. Les pouvoirs des agents de police administrative sont toujours allés de pair avec une définition de l'espace public où l'État reléguait la gestion de l'ordre assuré par les propriétaires sur des domaines privés de plus en plus étroitement circonscrits, et où ses agents ne pénétraient que sur invitation intérieure (réactivité) ou sur mandat extérieur d'un juge par exemple (proactivité). Les polices publiques ont ainsi occupé des portions de territoire public de plus en plus vastes que personne ne leur contestait¹⁸. Les polices administratives d'inspection, quant à elles, à qui sont octroyés des attributs de puissance publique et dont le nombre n'a cessé de croître¹⁹, sont autorisées à pénétrer sans être nécessairement invitées dans les entreprises pour y vérifier le respect de telle ou telle réglementation. Enfin la défense de l'inviolabilité du domicile, l'espace privé type, a toujours relevé du Code civil (article 9), du Code pénal (article 226-1) ou du Code de procédure pénale (article 59). Et personne n'a jamais songé, lors de la promulgation de la loi sur la vidéosurveillance, à évoquer l'idée que cette technique pouvait être utilisée par des entités privées dans leur propre espace « domestique » ou domaine privé. Il n'y a évidemment nul hasard en France à ce que la défense de l'intimité ou de la vie privée au sein du domicile soit définie en référence au droit public comme un « lieu fermé au public », alors qu'il aurait pu être défini au cours de l'histoire comme un espace ouvert à la famille, fût-elle élargie ou nucléaire, par exemple.

De fait, l'article 10 de la loi du 21 janvier 1995 n'apporte pas de véritables lumières sur la nature des espaces balayés par les caméras : il évoque la *voie publique* et *tous autres lieux et établissements particulièrement exposés à des risques d'agression ou de vol*²⁰. La seule précision que donne le texte à propos de la voie publique consiste à interdire aux caméras la possibilité de visualiser l'intérieur des immeubles d'habitation, ou plus spécifiquement leurs entrées. Bref, le législateur concède que le domicile est un espace privé pouvant s'étendre jusqu'à la voie publique ; en conséquence, il cherche à le protéger du regard policier à distance²¹. L'image du notable, rentrant chez lui, et surpris au côté d'une

17. A. STINCHCOMBE, « Institutions of Privacy in the Determination of Police Administrative Practice », *The American Journal of Sociology*, vol. LXIX, n° 2, 1963, p. 150-160.

18. Le « domaine public » affecté à « l'utilité publique » selon les catégories du droit administratif en vigueur : voies et places publiques, halles, jardins publics, équipements sportifs, parties communes des administrations, voire cimetières.

19. P. LASCUMES et C. BARBERGER, « De la sanction à l'injonction. "Le droit pénal administratif", comme expression du pluralisme des formes juridiques sanctionnatrices », *Revue de science criminelle et de droit pénal comparé*, n° 1, 1988, p. 45-65.

20. Il est question d'y assurer la « protection des bâtiments et installations publics et leurs abords, la sauvegarde des installations utiles à la défense nationale, la régulation du trafic routier, la constatation des infractions aux règles de la circulation, ou la prévention des atteintes à la sécurité des personnes et des biens dans des lieux particulièrement exposés à des risques d'agression ou de vol », et en dehors de la voie publique, tous autres « lieux et établissements particulièrement exposés à des risques d'agression ou de vol ».

21. C'est sans doute la raison pour laquelle le décret d'application prévoit que le responsable du système de vidéosurveillance doit joindre à sa demande un « plan masse des lieux montrant les bâtiments du pétitionnaire et, le cas échéant, ceux appartenant à des tiers qui se trouveraient dans le champ de vision des caméras, avec l'indication de leurs accès et de leurs ouvertures » (article 1-1). Si les auteurs de ce texte semblent pétris de bonnes intentions, sont-ils pour autant réalistes ? Est-il raisonnable d'imaginer par exemple que le responsable d'une police municipale fournira l'indication des accès et des ouvertures de tous les bâtiments entrant dans le champ de vision de plusieurs dizaines de caméras ?

maîtresse, constitue en général, dans la classe politique, le fantasme repoussoir le plus mobilisateur sur ce point. Ce sont surtout les « lieux et établissements privés ouverts au public » qui ont retenu l'attention, à partir du moment où l'on y fait une utilisation intensive d'agents privés de vigilance et de caméras de vidéosurveillance. Loin de constituer des *non-lieux* comme certains anthropologues aiment à les qualifier²², ces espaces ont des frontières mouvantes, parce qu'ils sont le théâtre de luttes de pouvoirs et d'appropriations différentielles opposant des propriétaires anonymes (maîtres des lieux gestionnaires sécurisant pour le compte de...) à des citoyens aux multiples facettes. Ces citoyens ont en effet la particularité d'endosser des statuts variés à mesure qu'ils pénètrent dans ces espaces pour y stationner, flâner, séjourner, aller et venir en tant qu'usagers, voyageurs, clients, consommateurs, salariés, malades, joueurs, supporters, etc. Ce qui n'est évidemment pas sans conséquence sur la nature de l'exercice de l'ordre, qui n'est plus nécessairement un ordre public. Au lieu d'inventer, comme le fit le juge américain Laskin, le concept de *propriété privée de masse* pour définir l'extension des espaces hybrides policés par des gardiens et des techniques payés par les maîtres des lieux auxquels le droit définit les obligations de faire ou de ne pas faire²³, la jurisprudence française est restée très abstraite à ce sujet. Elle se contente d'évoquer des « lieux accessibles à tous sans autorisation spéciale de quiconque, que l'accès en soit permanent et inconditionnel ou subordonné à certaines conditions, heures ou cause déterminées »²⁴. Aux sociologues d'imaginer alors quels sont ces lieux et de montrer comment ils sont effectivement policés. Les juristes pensent surtout aux lieux de travail, lieux ouverts à la communauté des seuls salariés et fermés aux autres²⁵, ou aux ERP (établissements recevant du public) soumis à des réglementations de sécurité spéciales, en matière de protection contre l'incendie notamment.

Mais cette catégorie juridique paraît de plus en plus inadaptée à la réalité de la gestion de la diversité des troubles qui s'y produisent, au point que des pressions sociales se font nettement sentir pour la faire éclater et la rendre plus adéquate à la gestion effective des différentes modalités de gestion de l'ordre (*policing*) rencontrées dans tel ou tel de ces espaces. Pour ne prendre que le cas de la gestion de l'ordre hospitalier, les hôpitaux publics ayant une vocation traditionnelle à ouvrir leurs portes à la souffrance et à la pauvreté extérieures se trouvent aujourd'hui dans l'obligation de protéger l'intimité des malades et la sécurité du personnel soignant contre ces mêmes populations tout venant. L'étroitesse de la notion d'ERP dont disposent les responsables de la sécurité pour agir est vécue comme une contrainte. Pire, comme une entrave qui leur donne le sentiment de se mouvoir dans ce qu'il est convenu d'appeler une forme d'insécurité juridique²⁶.

22. M. AUGE, *Non-lieux, introduction à une anthropologie de la surmodernité*, Paris, Seuil, 1992.

23. C.D. SHEARING et P.C. STENNING, « Private Security : Implications for Social Control », *Social Problems*, vol. 30, n° 5, 1983, p. 493-506.

24. Cour d'appel, Paris, 19 nov. 1986 confirmant un jugement du TGI de Paris du 23 octobre 1986, *Gazette du Palais*, 8 janvier 1987.

25. C. PETTITI, « Le droit de fouilles dans les entreprises et les locaux commerciaux », *La Semaine juridique*, n° 4, 25 janvier 1989, I : Doctrine, 3373. Voir également, M. GRÉVY, « Vidéosurveillance dans l'entreprise : un mode normal de contrôle des salariés ? », *Droit social*, n° 4, 1995, p. 329-332.

26. R. LE DOUSSAL, « À l'hôpital : anti-malveillance et technologies », *Les Cahiers de la sécurité intérieure*, n° 21, 1995, p. 75-87.

II. Les opérateurs de la vidéosurveillance

Curieusement, c'est la question la plus occultée de la loi examinée, alors qu'elle en constitue un enjeu essentiel. La loi prévoit que le responsable du système dépose une demande d'autorisation auprès de l'autorité préfectorale (article 10-III). Ce régime déclaratif est donc analogue à celui qu'avaient institué la loi de 1983 et les décrets de 1986 sur le contrôle préfectoral des entreprises de gardiennage, transports de fonds et protection des personnes ²⁷. Quant au récent décret d'application, il se contente de préciser à ce sujet quel doit être le contenu du dossier de demande pour ceux qui s'équiperont à l'avenir ou régulariseront leur dispositif : un rapport de présentation des finalités du projet, divers plans détaillés des lieux surveillés, les descriptions des dispositifs de vidéosurveillance ainsi que des mesures de sécurité pour la protection des images éventuellement enregistrées, les modalités d'information du public et du droit d'accès des personnes intéressées, ainsi que la désignation des personnes ou du service responsable de l'exploitation du système (article 1). Mais qui sont les personnes ou le service responsables de l'exploitation du système de vidéosurveillance ?

En dehors des propriétaires de salles de jeux dans l'obligation légale d'installer des systèmes de vidéosurveillance, on peut dire que sont virtuellement concernées par la nouvelle réglementation des milliers de personnes dirigeant un petit commerce muni par exemple d'une caméra visant l'espace de vente et d'un écran de contrôle au comptoir, auxquelles les assureurs ont suggéré qu'elles devraient s'en équiper, sous peine de voir leur prime risque vol et cambriolage augmenter ²⁸. Or il est à peu près certain que le contrôle préfectoral ne portera pas là-dessus, parce que les coûts en seraient exorbitants.

Au demeurant, qui définira, et selon quels critères, les lieux « particulièrement exposés à des risques d'agression ou de vol » ? On aurait pu penser que l'autorité préfectorale assistée des polices dussent au moins solliciter les organisations déjà équipées. Mais comme l'administration préfère toujours marcher à l'économie et au moindre coût, c'est la solution du régime déclaratif général qui jouera, ce qui la dédouanera de surcroît d'une quelconque responsabilité en cas de défaillance de la part du pétitionnaire concerné.

L'administration n'aura pas de mal, recherchant les « intentions du législateur » comme l'on dit, à solliciter les dirigeants des organisations les plus visibles : l'ensemble des chefs de police municipale et policiers municipaux affectés aux écrans de contrôle ; au sein des grandes surfaces, les chefs de poste des équipes de vigilance et agents affectés à la manipulation des caméras ou à l'observation sur les moniteurs (fonctions sous-traitées) ; ou bien, les chefs d'équipe internes (agents d'encadrement sala-

27. F. OCQUETEAU, « La consécration juridique et politique du secteur de la sécurité privée », *Actes. Les cahiers d'action juridique*, n° 60, 1987, p. 3-13.

28. F. OCQUETEAU, « Assurances et marché de la protection anti-malveillance », *Risques*, n° 16, 1993, p. 77-101.

29. On en décomptait environ quinze mille en 1991 ; cf. F. OCQUETEAU, 1987, *op. cit.* Désormais, tout agent et/ou dirigeant d'un service ou d'une équipe de gardiennage exerçant dans un établissement recevant du public (en sous-traitance ou en interne) est virtuellement concerné, car il est capable d'accomplir aujourd'hui sa mission derrière un écran de vidéosurveillance, ou comme rondier en connexion avec un opérateur vidéo.

30. Sur ce point, voir F. LUCHAIRE, « La vidéosurveillance et la fouille des voitures devant le Conseil constitutionnel », *Revue de droit public*, 1995, p. 575-597. Le décret d'application prévoit que la demande ou la déclaration et la mise en conformité du système doivent avoir lieu dans un délai de six mois à compter de la date de sa promulgation. Quant à l'autorité préfectorale, elle dispose d'un délai d'un an à compter du dépôt de la déclaration pour délivrer l'autorisation (article 18).

31. E. RICHARD, « La loi du 21 janvier 1995 : les conséquences pour l'entreprise », *Les Cahiers de la sécurité intérieure*, n° 24, 1996, p. 13-24.

32. J.P. THERON, « Commentaire de la loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité », *L'actualité administrative. Droit administratif*, n° 3, mars 1995, p. 207-211. Voir également, F. LAFAY, « Note sous Conseil constitutionnel, 18 janvier 1995 », *La Semaine juridique*, n° 44/45, 1^{er} novembre 1995, II : Jurisprudence, 22525.

33. Cf. L. CADOUX, « La vidéosurveillance dans les lieux publics et les lieux privés ouverts au public », *Après demain*, n° 376/377, 1995, p. 19-23.

riés) ; mais encore tout directeur et membre du service de sécurité interne à un ERP privé ou public tel qu'hôpital, banque, école, ou bâtiment administratif. Bref, des organisations somme toute aisées à répertorier dans la mesure où les casiers judiciaires des membres des « services de surveillance internes » à ces établissements furent en principe, dans la décennie passée, contrôlés par les services préfectoraux²⁹.

Il existe encore un flou persistant à propos des entreprises publiques (établissements publics industriels et commerciaux ; établissements publics administratifs et culturels) dont la vidéosurveillance est exercée par des agents de la police publique et de la gendarmerie nationale ou d'anciens militaires. À cet égard, les textes sont bruyamment muets, notamment au sujet des agents des services de vidéosurveillance, télé-surveillance et télé-sécurité de la Régie autonome des transports parisiens (RATP) par exemple, ou des agents du Service d'Information Sécurité de la Préfecture de police de Paris, etc.

Au fond, on est tenté de dire que la commission départementale instituée par la loi pour rendre un avis sur le dossier présenté par le pétitionnaire sera soumise à diverses modalités de transparence que, par définition, elle ne maîtrisera pas. Certes, la saisine du Conseil constitutionnel a provoqué l'obligation pour les préfets de répondre de façon expresse à toute candidature³⁰. Du coup, l'administration s'est sentie obligée de définir le plus restrictivement possible le champ d'application du texte. Pour autant, on peut douter du fait que la procédure imaginée par le gouvernement permettra de voir un « véritable dialogue [s'instaurer] entre le pétitionnaire et la commission », comme l'affirme un membre du cabinet du directeur général de la Police nationale³¹. À notre sens, le dialogue en question risque de tourner court, faute d'informations pour le nourrir. Le décret d'application décline en effet les hypothèses sous lesquelles le pétitionnaire pourra ne pas faire figurer dans le dossier de candidature les plans descriptifs de l'installation : un service de l'État pour des « raisons d'ordre public » (article 2), un opérateur privé ou public pour des « raisons impérieuses touchant à la sécurité des lieux où sont conservés des fonds ou valeurs, des objets d'art ou des objets précieux » (article 3), ou un établissement « intéressant la défense nationale » (article 4). Quant à l'obligation de tenir ces plans à disposition d'un membre de la commission qui pourra (mais personne ne l'y forcera) venir en prendre connaissance sur place, elle ne concerne que le pétitionnaire visé à l'article 3. C'est dire à quel point les restrictions sont nombreuses. Tout a déjà été dit par ailleurs sur cette commission « sous influence » avant même qu'elle ne soit mise en place³². Le Conseil constitutionnel ayant choisi de donner raison au gouvernement contre la Commission nationale de l'informatique et des libertés (CNIL), cette dernière s'est inclinée³³. Point n'est besoin

d'y revenir ici ³⁴. La question qui nous intéresse est plutôt la suivante. À supposer que les pétitionnaires soient correctement contrôlés et bien éduqués sur leurs droits et devoirs par l'administration préfectorale, que vont faire les agents opérateurs de l'information qu'ils vont visionner sur les écrans et enregistrer dans l'espace public ou dans l'espace privé ouvert au public ? La réponse est en réalité assez simple. Ils feront ce qu'ils faisaient auparavant, mais le plus légalement du monde, c'est-à-dire d'abord travailler au service des objectifs de l'organisation qui les emploie. Chercher la paix bancaire, la paix commerciale, la paix hospitalière, la paix scolaire, la fluidité des flux dans les espaces de transport, etc., avec les savoir-faire qui sont les leurs. Mais avec cette particularité supplémentaire que la recherche fonctionnelle de la paix, propre à l'espace des organisations en question, se fera désormais d'une façon plus contrainte qu'auparavant, puisqu'il leur faudra s'accommoder du regard des préfets, plutôt que de s'effaroucher de celui de citoyens particulièrement procéduriers. Ce qui veut dire que si la coopération ne s'institue pas spontanément de la part de qui devient un partenaire des autorités alors qu'il avait naguère plus d'autonomie, les polices publiques auront à leur disposition de nouveaux moyens de pression pour l'amener à composer avec elles.

III. Des finalités et des applications multiples

Que cherchent en réalité les dirigeants des organisations qui, poussés par les industriels et les marchands de sécurité, s'équipent de caméras de vidéosurveillance ? Comment réagissent-ils aux prescriptions de la loi censées apporter un peu plus de transparence qu'auparavant sur les enregistrements des images ? Quelques exemples tirés d'études empiriques vont nous permettre de répondre à ces questions, ou du moins d'en laisser entrevoir l'extrême richesse et complexité.

Dominique Boullier ³⁵ a montré par exemple à quel point les capteurs de la RATP déclenchant les images étaient inefficaces, parce qu'ils étaient réglés sur une définition type des comportements du délinquant. Ils s'inspirent largement du mode de surveillance nocturne des entreprises fermées, alors que, dans l'espace du métropolitain, le bruit et la foule ne permettent aucunement d'atteindre de tels objectifs exigeant *a priori* un environnement silencieux. Visant par ailleurs à détecter un délinquant en train de franchir des limites interdites ou de s'enfuir en courant après une agression, ou à détecter une victime par son appel au secours, ces présumés (courir, crier) rationalisent des situations ou des cas de figure théoriques qui sont en pratique exceptionnels ou inexistantes. De fait, il revient alors aux opérateurs de discriminer les événements et de lever le doute sur la cause du déclenche-

34. On relèvera simplement ceci : le décret dispose que l'autorité préfectorale invite expressément le pétitionnaire à s'adresser à la CNIL dans le cas où les informations fournies lors de la demande d'autorisation font apparaître que les enregistrements visuels seront utilisés pour la constitution d'un fichier nominatif (article 5). Cette concession de dernière minute à la CNIL est une fois de plus une manière habile de dédouaner la commission départementale de la responsabilité de cette question essentielle. Mais il aurait mieux valu préciser si l'abstention sur ce point était coupable, faute de quoi la portée de cette disposition se limiterait au pur symbole.

35. D. BOULLIER, « La vidéosurveillance à la RATP : un maillon controversé de la chaîne de production de sécurité », *Les Cahiers de la sécurité intérieure*, n° 21, 1995, p. 88-100.

ment de l'alarme. Les défaillances humaines étant à ce sujet très nombreuses, elles disqualifient les systèmes et conduisent alors la maintenance à mettre au point des dispositifs qui font transiter tous les incidents que l'on peut suivre sur les écrans vers un point central. Mais se pose alors un nouveau problème. Comment exploiter les informations concernant tous les incidents observés alors que les capacités d'intervention dont on dispose pour les faire cesser sont très limitées ? Comment trouver le bon endroit de l'incident, distinguer l'auteur de la victime, déterminer l'équipe disponible capable d'intervenir dans les temps avec les moyens adaptés ? À défaut d'y parvenir, la vidéosurveillance se voit alors assigner un objectif beaucoup plus modeste : suivre à distance l'équipe d'agents que l'on guide sur l'incident dans le but d'assurer leur propre sécurité.

De la même façon, nous avons montré ³⁶ que la vidéosurveillance dans les centres commerciaux, censée contribuer à la prise en flagrant délit de voleurs à l'étalage, n'avait d'efficacité que sous certaines conditions : uniquement dans le cas où les agents postés derrière les écrans restaient en contact étroit avec les agents de détection postés dans les rayons ; uniquement si elle était couplée à une logique d'interpellation et de négociation avec le ou les auteurs du délit dans une situation de rapport de force favorable, c'est-à-dire quand la densité des clients dans les rayons était plutôt clairsemée. La preuve par l'image joue plutôt comme une manière supplémentaire de protéger les agents interpellateurs d'éventuels comportements de rébellion, ou comme la preuve que la procédure de négociation ayant suivi l'interpellation n'a pas été accomplie sous la contrainte physique ou psychologique. Il faut savoir que la gestion de ces flagrants délits est devenue tellement monnaie courante dans les grandes surfaces qu'elle a été privatisée *de facto* depuis 1986 pour les opérateurs souhaitant recourir à la procédure de dépôt de plainte simplifiée. Les policiers négocient donc de plus en plus souvent avec les services de vigilance les affaires les plus sérieuses selon des critères définis préalablement (vol d'un montant élevé commis par un client inconnu, ou vol peu important mais réitéré, commis par un perturbateur notoire qui n'accepte pas de reconnaître ses torts). Dans les faits, impératifs du commerce — tout client est un voleur en puissance qu'on ne peut exclure que s'il est réellement insolvable ou récalcitrant — et impératifs de police — un bon voleur est un voleur dont on peut prouver qu'il est multirécidiviste et qu'il a quelque chance de faire l'objet d'une condamnation à l'emprisonnement — sont l'objet d'incessantes négociations avec de multiples intervenants, notamment dans les zones urbaines difficiles (parents, éducateurs, vigiles à l'interface de la prévention situationnelle et de la prévention sociale ³⁷). Quant aux enregistrements de vidéosurveillance, nous avons pu constater ³⁸ qu'ils étaient rarement conservés au delà de

36. F. OCQUETEAU et M.L. POTTIER, « Vidéosurveillance et gestion de l'insécurité dans un centre commercial : les leçons de l'observation », *Les Cahiers de la sécurité intérieure*, n° 21, 1995, p. 60-74.

37. Sur le rôle des « grands frères » par exemple, voir P. DURET, *Anthropologie de la fraternité dans les cités*, Paris, PUF, 1996.

38. E. HEILMANN et A. VITALIS, *Nouvelles technologies, nouvelles régulations ?* Strasbourg, Rapport Gersulp/Pirvilles/Ihesi, 1996.

la limite d'un mois prévue par la loi. En revanche, la reproduction sur papier d'images de voleurs à partir de ces enregistrements et la constitution de fichiers nominatifs alimentés par ces images sont des pratiques courantes dans les centres commerciaux³⁹. Or rien n'a été dit à leur sujet. Il est certain qu'au sein de ces établissements, la loi y est déjà presque regardée comme largement obsolète avant d'être entrée en vigueur puisqu'elle fait comme si la conservation de l'information, à partir de la vidéosurveillance, ne pouvait être assurée que sur support analogique. Ce qui procède évidemment d'une large méconnaissance des usages de ces technologies dans ces espaces.

Considérons encore la façon dont la vidéosurveillance est investie par les banques ou dans les écoles, au regard par exemple des nouvelles exigences d'information du public qui devra désormais toujours être averti du fait qu'il est sous l'œil de la caméra (article 10-II de la loi).

Dans le secteur bancaire, où les équipements de télésurveillance et de vidéosurveillance ont fait leur apparition dès le début des années 80, des enquêtés ont clairement fait état de leur opposition à cette nouvelle obligation⁴⁰. L'absence d'information à ce sujet peut signifier l'absence d'un véritable système de protection, donc orienter le passage à l'acte d'agresseurs éventuels vers des sites non équipés (agences ou guichets automatiques). La croyance en l'effet d'un déplacement de ce type de criminalité est compréhensible si l'on admet que ne pas informer s'inscrit dans une stratégie de dissuasion et non de prévention⁴¹. Mais dans les établissements bancaires cette stratégie est restée largement ignorée du législateur qui n'a prévu aucun aménagement du principe d'information obligatoire à l'intention des usagers⁴². Curieusement, les seules limites apportées à ce principe visent les membres, pourtant honorables, de la commission départementale auxquels on est fondé à ne communiquer que des informations limitées sur les installations (article 3). S'agirait-il d'une marque de défiance de principe à leur égard reposant sur la nécessité de prévenir leurs possibles indiscretions ?

Dans un contexte différent, une école privée d'enseignement technique, l'absence d'information des élèves et des parents sur l'emploi d'un dispositif de vidéosurveillance est conçue comme un élément essentiel du projet d'établissement défini par le directeur⁴³. Le dispositif technique concilie ici un double objectif :

42. On appréciera les éclaircissements (!) de la circulaire aux préfets sur ce point. Elle mentionne que toute caméra ne doit pas être systématiquement signalée en tant que telle « en particulier pour des raisons de sécurité (cas des banques ou des contrôles routiers) ». Faut-il alors entendre que les autres ont d'autres finalités et lesquelles ?... Elle ajoute dans cette hypothèse : « Il y a lieu de faire en sorte que dans tous les cas où une personne peut être filmée, elle soit en situation de s'y attendre et qu'ainsi elle y consente » [c'est nous qui soulignons].

43. E. HEILMANN et A. VITALIS, 1996, *op. cit.*

39. De même l'emploi d'un appareil polaroid est fréquent dans ces lieux. Ainsi par exemple, la pratique d'un modèle de plainte pour vol dans un magasin à libre-service montre qu'un auteur majeur ne pouvant justifier son identité peut accepter de se soumettre à la prise d'un cliché photographique polaroid, en exemplaire unique, après avoir donné son accord manuscrit dans les termes suivants : « Je ne désire pas être présenté aux services de police pour vérification de mon identité et j'accepte de me soumettre à la prise d'un cliché photographique » (Parquet de Lille, dans FORUM FRANÇAIS POUR LA SÉCURITÉ URBAINE, *Lieux sensibles et insécurité : les grandes surfaces*, Paris, siège social, 1996, p. 86-88). Dans notre enquête portant sur la gestion de 2 084 vols à l'étalage détectés en 1993, il ressortait que 71 % des affaires avaient été enterrées au stade de l'établissement de la procédure de dépôt de plainte simplifiée, quoique tous les renseignements sur les auteurs étaient restés dans les bordereaux rangés depuis des lustres dans des armoires, et s'accompagnaient parfois de ces fameuses photographies (F. OCQUETEAU et M.L. POTTIER, 1995, *op. cit.*).

40. E. HEILMANN et A. VITALIS, 1996, *op. cit.*

41. La dissuasion repose aussi sur l'effet d'ignorance inhibitrice de l'agresseur quant aux moyens réels dont dispose la proie convoitée pour parer à son attaque éventuelle.

sécuritaire (l'anti-intrusion après la fermeture de l'établissement, la prévention des vols et des dégradations, etc.) et éducatif (la régulation du comportement des élèves selon un principe d'autodiscipline). La vidéosurveillance y a remplacé les surveillants que l'on rencontre habituellement dans tous les établissements scolaires. Aucune caméra n'est cachée. N'importe qui (un visiteur, un élève) peut observer les images défilant sur les moniteurs de contrôle placés derrière le guichet d'accueil de l'école. Le chef d'établissement justifie sa réticence à informer élèves et parents des finalités du système par son souci d'éviter une possible surenchère de leur part en matière de demande de sécurité (par exemple, communication d'une bande pour confondre l'auteur du vol banal dont aurait été victime un élève, etc.). La discrétion lui sert à conserver une importante marge de manoeuvre quant à l'utilisation des informations enregistrées par les caméras.

Au delà du jugement que peut susciter cette expérience précise, on voit bien qu'une information trop « claire et permanente » sur la présence d'une caméra peut présenter un inconvénient majeur. Celui de figer cette technologie dans des pratiques trop rigidement définies à l'avance, alors que la nécessité du principe de publicité ainsi que son application moins dogmatique ou plus souple pourraient laisser bien souvent aux contrôleurs et aux contrôlés la faculté d'en discuter, sinon d'en négocier, les objectifs réels.

Conclusion

Au sortir de cet examen des enjeux de la régulation publique sur les usages, il nous paraît que le législateur n'a pas vraiment fait l'effort de réfléchir plus loin qu'à une simple opération de légalisation de l'existant. Aucune préoccupation ne l'a convaincu d'anticiper par exemple sur les pratiques de vidéosurveillance privée dans les domaines privés, alors que de telles pratiques se répandent un peu partout dans le monde. Théorisé par Oscar Newmann⁴⁴, « l'espace défendable » ou « l'espace dissuasif » par le biais de vigiles et de caméras électroniques protectrices, filtrant les entrées et les sorties des propriétaires et autres usagers légitimes (à distinguer des intrus indésirables), est en effet devenu l'objet d'une pratique courante dans des quartiers de Los Angeles, ou dans les « villes fortifiées » de l'Amérique centrale et du Sud ou de l'Afrique du Sud assaillies par des océans de pauvreté environnante. Cela correspond même pour les particuliers concernés à un nouveau style de vie⁴⁵. Mais tout se passe en France comme si cette réalité n'existait pas ou n'avait pas de raison d'advenir. Personne ne s'en inquiète, car la plupart des citoyens et leurs mandataires politiques partagent culturellement l'idée que la seule menace problématique

44. O. NEWMANN, *Defensible Space. Crime Prevention through Urban Design*, New York, Macmillan, 1972.

45. M. DAVIES, *City of Quartz : Excavating the Future in Los Angeles*, Londres, Verso, 1990. Voir aussi, R. LOPEZ, « Un nouvel apartheid social, hautes murailles pour villes riches », *Le Monde diplomatique*, mars 1996, p. 1 et 12.

est celle de *Big Brother* avec ses « miradors électroniques publics »⁴⁶.

Ce n'est pas tout. On est confronté aujourd'hui à des situations sociales où la question de l'utilisation généralisée et diffuse de la caméra pourrait bien avoir des effets fort désagréables chez ceux-là même dont on prétend rentabiliser l'efficacité professionnelle. N'a-t-on pas vu récemment des vidéo amateurs filmer des policiers brutalisant des gens sur la voie publique ou dans des caves, et vu un préfet obligé de s'excuser du comportement de ses agents face au spectacle, relayé par les médias, des images enregistrées de leurs agissements ? Il ne s'agissait certes plus là de caméras de vidéosurveillance en circuit fermé. Pour autant, il n'en demeure pas moins légitime de se poser la question suivante : n'est-on pas, dans cette hypothèse, en présence d'un outil virtuel de « sécurité par incidence » qui pourrait fort bien se retourner contre la police, si des justiciers amateurs se mettaient à filmer systématiquement des pratiques dont il lui déplairait à la longue assez fortement qu'elles soient systématiquement rendues publiques ?

Enfin, les études empiriques dont nous avons fait état montrent que les finalités, déclarées ou latentes, des techniques de recueil d'information couplées à l'image sont innombrables pour les utilisateurs, les opérateurs publics ou privés et les usagers. Nous ne voulons pas dire qu'aucune régulation de l'État n'est possible ni souhaitable — à supposer même qu'on s'aperçoive de sa disqualification avant son entrée en vigueur —, bien au contraire, car le besoin de définir les règles du jeu et de les normaliser dans ce domaine demeure essentiel. Nous disons plutôt que l'actuelle légalisation des techniques de vidéosurveillance, en dépit de ses usages multiples et en dépit d'une concession de pure forme sur l'information du public vidéosurveillé, vise surtout autre chose : la maximalisation de l'information des « polices publiques de proximité » par les opérateurs des organisations ou, ce qui revient au même, la maximalisation de l'efficacité des organisations dans la gestion de leur ordre intérieur qui, s'il n'est pas sécuritaire par nature, doit néanmoins le devenir, puisqu'il doit aussi s'efforcer de s'adapter aux besoins et exigences professionnelles de la police publique. En effet, les techniques d'ilotage urbain, publiquement valorisées, échouent en France à satisfaire les effets escomptés pour des raisons autant historiques, organisationnelles que professionnelles⁴⁷. Et les polices concernées commencent à souffrir d'un certain discrédit, car elles ne parviennent pas à résoudre les problèmes d'insécurité vécus au quotidien, dans les délais les plus brefs, ou du moins à les empêcher de s'envenimer. Les gardiens de la paix sont alors de plus en plus ouvertement condamnés à feindre d'être les organisateurs d'un « partenariat » dont ils dicteraient les objectifs (la protection des personnes et des biens) à ceux qui

46. Pour reprendre une expression pour le moins douteuse ; cf. A. DE LAJARTE, 1996, *op. cit.*

47. D. MONJARDET, *Ce que fait la police. Sociologie de la force publique*, Paris, La Découverte, 1996.

disposent des moyens humains et technologiques de protection et de prévention des troubles. Ces derniers ne sont considérés avec amitié que dans la mesure où ils savent se plier à cette logique, celle de leur capacité à rendre des services de nature judiciaire et administrative : la police a besoin de preuves sur l'identité de délinquants, certes, mais elle a également besoin de se faire une religion sur les situations « à risque » qui ne se passent plus nécessairement dans la rue.

Quant aux usagers (et) délinquants virtuels filmés dans les espaces intermédiaires, la leçon qu'ils peuvent tirer de cette opération symbolique de restauration de l'autorité de l'État par la légalisation de la vidéosurveillance tient en peu de mots : qu'ils se débrouillent pour ou contre la conservation de leur image avec les maigres moyens que vont leur donner les nouvelles AANI (Autorités administratives non indépendantes), en jouant par exemple avec les juges sur d'éventuels conflits d'intérêt entre opérateurs publics et privés, ou tout simplement sur les failles de dispositifs qui ne seront jamais exactement adaptés aux exigences des situations, quel qu'en soit le degré de sophistication.