Retour sur la question du droit à l'image pour les Etats

Ou comment anticiper « Etat belge / Ministre de la Défense contre Google Inc. » ?

Jean-François Mayence, Lic. DES
Conseiller juridique « Relations internationales »
BELSPO

Fin septembre 2018, la presse internationale[1] rapportait l'intention du Ministre belge de la Défense, Steven Vandeput, de porter plainte contre Google Inc. afin de contraindre le géant américain à dégrader la résolution d'images de sites militaires belges qu'il publie sur Internet, notamment via ses applications intégrées Google Earth™ et Google Street View™. Cette nouvelle faisait suite à plusieurs articles de presse publiés entre décembre 2015 et janvier 2018 qui rapportaient une demande formelle du Ministre de « flouter » les images en cause. En réponse, Google avait indiqué avoir déjà flouté les prises de vues des rues autour des domaines concernés sur Google Street View, mais ne pas avoir pu faire de même pour les images sur Google Earth étant donné qu'il s'agissait de prises de vues aériennes dont Google n'était pas à l'origine[2]. La firme américaine n'est pas entrée dans le détail juridique de cette explication, mais on peut s'interroger sur l'incapacité technique d'un éditeur à intervenir sur des images qu'il publie en ligne afin de se conformer aux législations des pays représentés. D'autant que Google a, par le passé, donné droit à plusieurs requêtes gouvernementales et « pixellisé » des vues portant sur des sites sensibles. La question se pose donc de savoir de quels moyens – du moins juridiques – l'Etat belge dispose pour contraindre Google à obtempérer.

Nous proposons une brève synthèse de l'état de la question : les Etats jouissent-ils d'un droit à l'image pour censurer la publication de vues indiscrètes de leur territoire ? Cette question se pose en particulier pour les données satellitaires qui offrent une vision de plus en plus exhaustive de notre planète, dans son ensemble comme dans ses moindres détails. Notre propos se limitera donc à passer en revue les instruments susceptibles d'être invoqués par les Etats pour protéger leur « intimité » au regard de ces insaisissables espions.

Les technologies satellitaires d'observation de la Terre

(a) Différences entre prises de vue par satellite et prises de vue par aéronef

Ces différences s'expriment à la fois en termes juridiques (le régime applicable à l'opération des aéronefs au-dessus d'un territoire étatique devant être rapporté à celui applicable à l'opération de satellites en orbite) et en termes économiques (le coût marginal de l'image aérienne au m² étant supérieur à celui calculé sur la durée de vie opérationnelle d'un satellite).

[1] Cf. www.lesoir.be, 28/09/2018 ; www.usnews.com, 28/09/2018 ; www.bbc.com, 28/09/2018 ; etc.
[2] Cf. Belga 05/01/2018.

Les prises de vues de la Terre ont différentes sources possibles. Chacune d'elles est soumise à un régime juridique particulier. Il existe des prises de vues depuis le sol, qui vont de la photo du touriste de passage à celle prise par la voiture Google qui « scanne » les rues de nos cités et de nos campagnes pour en reproduire fidèlement l'image tridimensionnelle sur Internet. Il y a ensuite les prises de vues verticales, réalisées depuis un avion en vol, un drone ou un ballon. Plus l'altitude est élevée, plus la zone couverte est grande. Se pose alors la question de la résolution de l'image qui déterminera le niveau de détails visibles. C'est cette question qui fait principalement l'objet de la maîtrise, par un Etat, de l'image de son territoire et des caractéristiques de celui-ci. Cette maîtrise représente un enjeu stratégique à plusieurs égards : on pense à la protection d'infrastructures ou de sites sensibles, à celle des ressources naturelles, à celle de la tranquillité publique et du droit à la vie privée, ou encore, plus généralement, à la protection de l'ordre public contre toute forme d'intrusion plus ou moins malveillante[3].

Les photos prises depuis des aéronefs, y compris ceux téléguidés depuis le sol, sont sans doute les moins difficiles à réguler. L'occupation et l'utilisation de l'espace aérien fait l'objet, dans tous les pays, de conditions strictes et d'une surveillance constante. En outre, un aéronef ne se déplace pas comme un simple passant muni d'un appareil photo ou d'une caméra et qui peut se rendre difficilement identifiable ou saisissable. La prise de vue aérienne tombe directement dans le champ de contrôle de l'Etat, tant de par son objet (le territoire national) que de par son origine (l'espace aérien). Il est donc théoriquement possible d'empêcher la prise de vue de certaines parties du territoire national, soit en en interdisant le survol, soit en en interdisant la photographie depuis un aéronef en vol.

La situation est fondamentalement différente lorsque l'engin d'observation évolue dans l'espace extra-atmosphérique[4]. Cet espace n'est pas défini par le droit international qui, toutefois, le distingue de l'espace aérien d'un point de vue fonctionnel. Le long débat sur la délimitation entre espace aérien et espace extra-atmosphérique n'est pas notre propos ici. Nous nous bornerons à relever qu'un objet en orbite terrestre est unanimement considéré comme évoluant dans l'espace extra-atmosphérique (même si la question demeure pertinente de savoir si certains engins capables de passer d'un vol en mode aéronef à un vol orbital, et vice-versa, ne changent pas de régime juridique au cours de leur opération). Le droit international, tant conventionnel que coutumier, a consacré le principe de liberté et de non-appropriabilité de l'espace extra-atmosphérique[5]. Ceci implique qu'aucun Etat « survolé » ne peut intervenir pour interdire ou réguler l'activité d'observation. Seul l'Etat d'immatriculation du satellite dispose de ce pouvoir[6].

Jusqu'à la fin du XX^{ème} siècle, le statut particulier de l'espace extra-atmosphérique incitait plutôt les Etats à rechercher la coopération afin de renforcer la protection de leurs intérêts stratégiques. Bien entendu, l'Espace demeurait un terrain de manœuvres de choix pour la défense nationale, mais les gouvernements se montraient relativement discrets à ce propos, évitant les provocations inutiles. L'adjectif « militaire » ne faisait pas partie du vocabulaire diplomatique spatial, même si cette réalité n'était pas contestée. C'était sans compter l'avènement de la *New Space Economy* et de modèles économiques inédits, portés par le charisme d'entrepreneurs tels qu'Elon Musk ou Jeff Bezos. Leur

[3] Pour une analyse approfondie de l'utilisation des images satellitaires dans un context socio-politique, voyez notamment BAKER, JC, WILLIAMSON, RA, *Satellite Imagery Activism: Sharpening the Focus on Tropical Deforestation*, in Singapore Journal of Tropical Geography, 27 (2006), pp. 4 à 14. L'image satellitaire à des fins humanitaires ou de propagande d'Etat a franchi une étape décisive dans son intégration culturelle avec son usage en 1995 pour révéler les massacres perpétrés dans le cadre du conflit bosniaque et les charniers de Srebrenica. L'instrumentalisation par le Gouvernement américain reposait sur le moment de la publication des données satellitaires et sur la distance que ces observations impliquaient, faisant des Etats-Unis un « témoin impuissant » de ce crime (voyez PARKS, L., *Satellite Views of Srebrenica : Tele-Visuality and the Politics of Witnessing*, in Social Identities 7 (4), pp. 585 à 611).
[4] « *Outer space* » en anglais.
[5] Voyez Articles I et II du Traité des Nations Unies sur les Principes régissant les Activités des Etats en matière d'Exploration et d'Utilisation de l'Espace extra-atmosphérique, y compris la Lune et les autres Corps célestes, du 27 janvier 1967.
[6] Voyez Article VIII du même traité.

stratégie – ou du moins leur communication – repose sur la politique du fait accompli : « J'y suis, j'y reste ». Outre leurs impressionnantes fortunes personnelles et les capitaux de leurs sociétés, ils peuvent compter sur la clientèle fidèle et généreuse des agences publiques. Mais surtout, ils ne lisent dans les traités internationaux aucune restriction à leur *business plan*, et à raison : seuls les Etats sont assujettis à ce droit international né de la Guerre froide. Le temps que les Administrations mettent en place un carcan réglementaire idoine à leurs projets, ils les ont imposés comme une évidence au son du *buzz* des réseaux sociaux et de la presse en ligne.

Un contexte particulier : les prémices d'une nouvelle « Guerre des Etoiles »

Si cette liberté de l'Espace a permis les plus grands exploits du XX^{ème} siècle et l'avènement de la société numérique telle que nous la connaissons au XXI^{ème}, elle pose aujourd'hui le risque de voir certaines nations déployer en orbite un véritable arsenal anti-satellite. Car l'impossibilité de contrôle juridique par l'Etat survolé conjuguée à la capacité de détection sans cesse croissante des charges utiles[7] a le don de rendre les gouvernements paranoïaques. La solution radicale consistant à détruire ou à neutraliser en orbite l'œil espion est donc de moins en moins hypothétique : les politiques spatiales nationales intègrent de plus en plus la nécessité de doter leurs systèmes orbitaux de moyens de défense, poussant ainsi à une surenchère qui contraste avec l'esprit des traités internationaux. La récente annonce, par le Président Trump[8], de la constitution d'un corps d'armée dédié à la défense spatiale en est l'illustration par excellence. Plus encore, cette nouvelle dimension sécuritaire de l'utilisation de l'Espace s'inscrit dans une préoccupation globale qui est celle de la viabilité à long terme des activités spatiales. Cette viabilité intègre des éléments de « sécurité » (tant dans le sens anglais de « *security* » que dans celui de « *safety* »). Ainsi, la réduction des débris spatiaux qui constituent une nuisance majeure pour l'utilisation des orbites terrestres fait partie des enjeux discutés par les Etats dans diverses enceintes multilatérales. L'une des solutions envisagées, à côté de celles visant à réduire a priori la production de tels débris, est l'évacuation de débris existants au moyen de systèmes de capture (aimants, filets, etc.). Ce type de solutions – *Active Debris Removal (ADR)* – donne du fil à retordre aux juristes en ce qu'elle suppose la capacité technique pour un Etat de capturer et de détruire un satellite soumis à une juridiction étrangère. Certes, la notion de « débris spatial » ne fait l'objet d'aucune définition en droit international, mais c'est surtout la difficulté de surveiller en temps réel ce qui se passe en orbite qui rend les gouvernements nerveux. Un satellite par trop curieux pourrait ainsi disparaître sans crier gare, harponné par un autre engin ou neutralisé par une décharge électromagnétique. Tout ceci explique l'importance de parvenir à des solutions consensuelles, en matière d'exploitation de systèmes d'observation de la Terre, à commencer par la publication et l'accès aux données. Car à l'espionnage d'Etat (qui dispose le plus souvent de capacités militaires propres) s'ajoute aujourd'hui la menace terroriste ou anti-gouvernementale : pour elle, les données Google Earth sont du pain bénit. En outre, l'accès libre à ces données par le grand public décrédibilise les efforts visant à construire une culture de la sécurité, y compris dans les sphères privées.

(b) Intégration et traitement des données

L'imagerie satellitaire, même si ce n'est pas là une caractéristique qui lui est exclusive, repose sur l'utilisation quelquefois combinée de différentes technologies. On distingue principalement l'imagerie optique de l'imagerie radar. La différence fondamentale réside dans le fait que les technologies optiques captent la lumière générée ou réfléchie par l'objet observé, tandis que les technologies radar génèrent leur propre « éclairage » qu'elles envoient sur l'objet observé. Il s'agit en réalité d'un signal

[7] Instruments fonctionnels embarqués à bord du satellite (caméra, senseur, transpondeur, etc.).
[8] Cf. H.R.2810 et S.1519 - *National Defense Authorization Act for Fiscal Year 2018* (disponible sur www.congress.gov).

électromagnétique d'une longueur d'onde spécifique. Ceci explique que les radars peuvent observer un objet même lorsque celui-ci et plongé dans l'obscurité ou caché par des nuages. En schématisant, le radar détecte les reliefs (c'est-à-dire les formes susceptibles de lui renvoyer le signal électromagnétique). La technologie optique, quant elle, permet d'observer l'objet en fonction de la fréquence de lumière qu'il renvoie et de distinguer ainsi les zones de végétation des zones urbaines, les zones de chaleur des zones froides, etc.

Outre ces modulations, l'imagerie satellitaire est le résultat de la combinaison de données de natures variées (métadonnées) : à la donnée optique ou radar s'ajoutent des données relatives au positionnement et au temps : le satellite, de par son passage régulier et systématique au-dessus d'un même point, peut observer l'évolution spatio-temporelle d'une situation. Des relevés au sol peuvent également compléter ou valider les données spatiales. On parle d'applications intégrées pour désigner cette combinaison de produits (traditionnellement observation, positionnement et télécommunication).

Enfin, la disponibilité de l'image satellitaire conjuguée au traitement des méga-données (*big data*) offre un potentiel impressionnant d'information de masse que les gouvernements peinent – c'est un euphémisme – à réguler. En l'absence d'un instrument juridique global encadrant les outils de la société de l'information, on voit mal la pertinence d'accords ponctuels portant sur les flux de données spécifiques limités à quelques Etats. Les solutions juridiques, dans un cas comme celui qui implique le Ministère belge de la Défense et Google, passent par des réflexions et des actions ad hoc.

Le cadre juridique de la diffusion des données satellitaires d'observation de la Terre

(a) Le cadre juridique international

Le cadre juridique international qui s'applique aux activités d'observation de la Terre par satellite et à l'accès aux données résultantes est difficile à définir. Tout d'abord, parce qu'il n'existe que peu de sources internationales propres à ce domaine (pas de traité, pas de jurisprudence internationale), ensuite parce que, de par leur nature, les activités satellitaires d'observation de la Terre sont soit soumises aux lois nationales, soit affectées par elles. Le droit interne a donc un impact transfrontalier qu'il convient d'appréhender au cas par cas, ce qui n'est pas chose aisée. D'autant que peuvent interférer dans l'analyse juridique des éléments de nature politique qui, par définition, restent à la discrétion des Etats concernés.

Il faut néanmoins distinguer les différentes raisons pour lesquelles un Etat cherche à garder la maîtrise de l'image de son territoire. Il s'agit principalement (1°) de la protection des ressources naturelles et (2°) de la sécurité à travers la protection des sites qualifiés de « sensibles » ainsi que des activités qui y sont menées.

(i) Premier paradigme : la protection des ressources naturelles

Le droit souverain des peuples à jouir de leurs ressources naturelles a été consacré à maintes reprises comme l'un des plus fondamentaux qui soient. D'abord, par la Résolution de l'Assemblée Générale des Nations Unies 1803 (XVII) adoptée le 14 décembre 1962 selon laquelle « *la prospection, la mise en valeur et la disposition [des ressources naturelles] ainsi que de l'importation des capitaux étrangers nécessaires à ces fins devraient être conformes aux règles et conditions que les peuples et nations considèrent en toute liberté comme nécessaires ou souhaitables pour ce qui est d'autoriser, de limiter ou d'interdire ces activités* ».

Cette haute recommandation est ensuite reprise et gravée dans le marbre de la loi internationale par les pactes jumeaux de 1966[9] qui partagent la même disposition, mot pour mot : « *Pour atteindre leurs fins, tous les peuples peuvent disposer librement de leurs richesses et de leurs ressources naturelles, sans préjudice des obligations qui découlent de la coopération économique internationale, fondée sur le principe de l'intérêt mutuel, et du droit international. En aucun cas, un peuple ne pourra être privé de ses propres moyens de subsistance.* »

Ce volet « passif » de la protection des ressources naturelles laisse toutefois les Etats démunis d'actions concrètes visant à protéger les ressources naturelles de leur territoire. Longtemps les moyens satellitaires – qui, encore une fois, dispensent leur utilisateur de toute permission de la part de l'Etat survolé – sont restés dans les mains de puissants opérateurs économiques et ont servi une nouvelle forme de colonisation. Sans réellement connaître la nature et l'importance exactes des richesses qu'ils bradaient, des gouvernements de pays en voie de développement, quelquefois corrompus, ont concédé l'exploitation de sites naturels à des firmes industrielles étrangères. La maîtrise de l'information géospatiale a permis à certains de ces exploitants de mettre la main, pour une contrepartie disproportionnée, voire léonine, sur un patrimoine national[10]. Ceci alors que les mêmes images satellitaires étaient susceptibles de fournir de précieux renseignement sur l'impact que de telles activités auraient (et ont eu) sur l'environnement, ressource naturelle par excellence.

De ce constat et de cette préoccupation est née l'initiative de l'UNCOPUOS[11] qui, en 1986, a abouti à l'adoption, par l'Assemblée Générale des Nations Unies d'une Résolution sur les Principes sur la Télédétection[12]. A première vue, cette résolution semble réaffirmer les principes consacrés par le Traité des Nations Unies sur l'Espace de 1967 en se focalisant sur un type d'activité spécifique : la télédétection. En réalité, la Résolution de 1986 va bien plus loin.

De par son objet, la Résolution déborde du cadre traditionnel du droit des activités spatiales (au sens d'activités opérationnelles menées ***dans*** l'espace extra-atmosphérique). Les activités considérées sont en effet définies comme les « *activités d'exploitation des systèmes de télédétection spatiale, des stations de réception et d'archivage des données primaires, ainsi que les activités de traitement, d'interprétation et de distribution des données traitées* ». Cette définition est toutefois limitée aux données collectées à des fins de gestion des ressources naturelles ou de protection de l'environnement (cf. définition de la « télédétection »), ou encore de prévention ou de gestion des catastrophes naturelles (Principe XI). Les Principes adoptés par l'Assemblée Générale des Nations Unies portent donc non seulement sur la captation, par l'instrument satellitaire, de la donnée d'observation de la Terre, mais également sur son traitement et son exploitation via le segment « terrestre » de la chaîne menant au produit final. C'est donc une incursion du droit de l'Espace dans un domaine économique impliquant des acteurs non-spatiaux. De là le caractère exorbitant de la Résolution qui, sous prétexte de réaffirmer les principes du bénéfice pour l'humanité (Principe II), du respect de la souveraineté de l'Etat sur ses ressources naturelles (Principe IV) ou encore de la responsabilité internationale des Etats du fait de leurs activités spatiales (Principe XIV), entend réguler la diffusion et l'utilisation des données et des produits dérivés.

Si la Résolution de 1986 ne constitue pas un instrument juridique liant, c'est-à-dire générant des droits et des obligations pour les Etats, il n'en demeure pas moins qu'elle met en place un mécanisme concret et détaillé permettant l'accès aux données d'observation de la Terre (Principe XII), au point

[9] Pacte international relative aux droits civils et politiques et Pacte international relatif aux droits économiques, sociaux et culturels, faits à New york, le 16 décembre 1966
[10] Voyez à ce sujet : KRAFFT, S., *In Search of a Legal Framework for the Remote Sensing of the Earth from Outer Space*, in Boston College International & Comparative Law Review, Vol. 4 , Issue 2, Art. 6 (1981), p. 453 et suiv.
[11] Comité des Nations Unies pour les Utilisations pacifiques de l'Espace extra-atmosphérique
[12] UNGA Res. 41/65, 3 décembre 1986

que ce mécanisme fait partie intégrante de la pratique des Etats dans ce domaine. Aux termes de cette disposition, tout Etat observé a accès, sans discrimination et à des conditions de prix raisonnables, aux données traitées concernant le territoire relevant de sa juridiction. Il en va de même des informations analysées disponibles, à ceci près que seules les informations en possession de l'Etat opérant le système satellitaire sont concernées (excluant donc les informations produites et détenues par des opérateurs non-gouvernementaux). Encore une fois, les données d'observation militaire ou destinées à d'autres fins, comme la vérification de traités, ne tombent pas dans le champ de la Résolution.

Sans qu'elle soit explicitement citée comme référence, la Résolution de 1986 peut être considérée comme à l'origine de nombreuses politiques gouvernementales ou intergouvernementales visant à mettre à disposition des utilisateurs du monde entier des données satellitaires à des fins environnementales ou économiques. C'est le cas notamment des programmes civils d'observation de la Terre européen (ESA, Union européenne) et américain (NASA, NOAA). On peut donc considérer que la pratique des Etats dépasse dans une certaine mesure les principes édictés par les Nations Unies.

On en conclura cependant qu'en dehors de l'exploitation de ses propres satellites gouvernementaux, la protection des ressources naturelles ne permet aucunement de garantir à l'Etat l'exclusivité des données se rapportant à son territoire.

(ii) Second paradigme : la protection des sites sensibles

Voir sans être vu : de paradoxe à paradigme

Il est un fait que la souveraineté de l'Etat repose, du moins dans la conscience collective, sur la maîtrise qu'il exerce ou est susceptible d'exercer sur son territoire, y compris jusqu'à ses confins les plus reculés. La maîtrise implique le contrôle et le contrôle requiert la vision. L'outil satellitaire est donc particulièrement apprécié par les gouvernements lorsque, dans leurs mains, il offre une vue modulable de l'empire de leur pouvoir. Inversement, le même outil se transforme en arme lorsqu'il permet l'intrusion d'une puissance étrangère ou l'organisation d'un complot terroriste. L'enjeu glisse ainsi de la maîtrise technologique à celle de l'information.

Se cacher du satellite n'est pas chose aisée. Certaines structures au sol peuvent être construites afin de camoufler un site, ou celui-ci peut être enfoui sous terre, mais le satellite a l'œil perçant et les algorithmes permettent d'analyser les images afin d'y détecter les anomalies. Reste donc à s'assurer la maîtrise de la diffusion de ces données.

La Belgique est loin d'être le premier Etat à se plaindre de l'indiscrétion de Google Earth. La Chine en a fait une menace contre sa sécurité nationale. D'autres Etats, comme l'Inde, se sont plaints de la publication de prises de vue de sites nationaux stratégiques et ont obtenu le floutage de certaines de ces images par Google[13]. Ces interventions de Google ont été décidées de commun accord avec les autorités nationales concernées. Il est difficile de déterminer dans quelle mesure des arguments de nature juridique ont été avancés par les Etats demandeurs, et, dans l'affirmative, lesquels. Google a évidemment tout intérêt à garder la maîtrise de ses données, ce qui nécessite un savant dosage entre conciliation et défense de ses prérogatives. Toujours est-il qu'en l'absence de cadre juridique international spécifique, Google joue de sa toute-puissance. C'est sans doute l'une des raisons qui ont poussé le Gouvernement chinois à lancer fin 2010 son propre service d'imagerie et de cartographie satellitaires (en.tianditu.com) : s'attaquer à l'hégémonie de Google tout en affichant sa vision officielle du monde chinois.

[13] Voyez *Google agrees to blur pix of key Indian sites*, TNN, *The Times of India*, 4 février 2007.

Sans doute la Belgique dispose-t-elle de moyens de pression politique pour agir sur une grande firme d'un pays membre l'OTAN, mais il ne faut pas surestimer le pouvoir du Gouvernement américain sur les géants du Net[14], d'autant qu'une attitude sélective et arbitraire dictée par les seules affinités politiques aurait pour effet d'user la fiabilité du produit Google.

Origine et vocation militaires des applications satellitaires de précision

Le paradoxe mis en lumière plus haut est en réalité une réminiscence de l'origine militaire des technologies d'observation de la Terre à haute et très haute résolution. Cette origine supposait au départ un accès exclusif et classifié aux données[15]. Avec la commercialisation de ce type de produits, tout comme ce fut le cas pour le GPS, le caractère exclusif s'est mué en une politique de libre accès et d'applications multiples que les autorités gouvernementales ont elles-mêmes encouragée, sans se soucier réellement des moyens de la contenir eu égard aux intérêts stratégiques nationaux. On comprend donc la préoccupation des experts en sécurité, premiers à réaliser les possibilités d'utilisations malveillantes des données de haute précision.

Toujours est-il que, dans l'arsenal juridique à la disposition des Etats pour réguler les activités spatiales non-gouvernementales, il existe certains moyens de limiter les capacités d'observation à la source. L'Article VI du Traité des Nations Unies sur l'Espace de 1967 impose aux Etats de soumettre à leur autorisation et à leur supervision continue lesdites activités. Il est donc loisible à un Etat, en conformité avec sa loi interne, de restreindre l'autorisation de lancement ou d'opération d'un satellite d'observation de la Terre à une capacité de résolution maximale[16].

(b) Le cadre juridique européen et national

(i) La Directive INSPIRE et la loi du 15 décembre 2011

La Directive 2002/2/CE du Parlement européen et du Conseil établissant une infrastructure d'information géographique dans la Communauté européenne (Directive INSPIRE) a été adoptée le 14 mars 2007 afin de doter la Communauté et ses Etats membres d'un soutien à leurs politiques sectorielles sous la forme d'informations géographiques systématisées et intégrées au sein d'une « infrastructure » unique. La finalité de cet instrument est donc bien d'optimiser l'accès aux données et leur utilisation à des fins diverses, institutionnelles, scientifiques, voire privées, par le biais des métadonnées, de l'interopérabilité, des réseaux et du partage.

La Directive INSPIRE n'a donc pas pour but de restreindre la diffusion des données d'observation satellitaire, tout au contraire. Elle est néanmoins intéressante dans le cas qui nous occupe en ce qu'elle prévoit un régime d'exception à l'accès public auxdites données. Parmi les exceptions, le fait qu'un tel accès nuirait aux relations internationales, à la sécurité publique ou à la défense nationale[17].

La Directive INSPIRE a été transposée en droit belge par une loi du 15 décembre 2011 qui prévoit en son article 9, §1er, que l'accès public aux données peut être restreint lorsqu'un tel accès nuirait à la

[14] D'autant que le Gouvernement américain a lui-même fort à faire pour protéger ses propres sites sensibles de satellites toujours plus performants. Voyez la requête introduite par DigitalGlobe en 1999 pour la commercialisation de données de 25 cm de résolution. L'autorisation délivrée en définitive limitait cette résolution à 50 cm (cf. SCOLES S., *How the Government Controls Sensitive Satellite Data*, Wired.com - 02/08/2018).
[15] PERKINS, C, DODGE M., *Satellite Imagery and the Spectacle of Secret Spaces*, in Geoforum (2009).
[16] Voyez l'exemple de DigitalGlobe à la note de bas de page ci-dessus.
[17] Cf. article 13.1 de la Directive.

sécurité publique, à la défense nationale, ou au caractère confidentiel des relations fédérales[18] internationales de la Belgique ou des relations de la Belgique avec les institutions supranationales.

(ii) La proposition de Directive sur les données satellitaires commerciales

Le 17 juin 2014, la Commission européenne publiait une proposition de directive relative à la diffusion de données satellitaires d'observation de la Terre à des fins commerciales. Ce projet visait à garantir la libre circulation et la libre diffusion des données satellitaires dans le marché européen, moyennant certaines garanties, notamment en matière de sécurité. L'économie générale de la directive en projet reposait sur une double distinction entre données satellitaires : d'une part entre celles à haute résolution et les autres, d'autre part entre diffusion sensible et autre diffusion. La directive proposée aurait instauré un régime à trois degrés, le premier degré garantissant la libre circulation et la libre diffusion des données hors haute résolution dans l'Union, le deuxième degré soumettant à une procédure nationale de vérification préliminaire les données à haute résolution et le troisième degré soumettant à un régime d'autorisation nationale les données à haute résolution et à diffusion sensible. La proposition de directive prévoyait également de faire échec aux obstacles à la libre circulation et à la libre diffusion de données produites par des systèmes satellitaires exploités hors de l'Union pour autant que l'Etat membre du fournisseur de ces données dans l'Union ait autorisé cette circulation et cette diffusion et les maintienne sous sa surveillance effective.

Rapidement, cette proposition de directive fit l'objet de critiques de la part des rapporteurs au Parlement européen. Mais c'est la Commission elle-même qui porta le coup de grâce en soulevant trois difficultés liées à sa proposition :

1. les restrictions liées à la sécurité imposées par les Etats membres,
2. les menaces pesant sur la sécurité de l'Union et liées à la diffusion non-contrôlée de données,
3. la nature hybride, en termes de compétences, des échanges de données appelant une coopération entre Etats membres.

Il se peut en outre qu'un autre argument moins explicite ait conduit la Commission à renoncer à son projet législatif. La base juridique de la directive proposée était l'Article 114 du Traité sur le Fonctionnement de l'Union européenne, première disposition du chapitre relatif au rapprochement des législations (en vue d'assurer le bon fonctionnement du marché intérieur). La Commission s'est bien évidemment gardée de viser l'Article 189 du même traité, relatif à la Politique spatiale européenne, puisque cette disposition exclut expressément toute harmonisation des législations nationales dans le domaine de l'espace extra-atmosphérique. Cette prudence démontre néanmoins la volonté de la Commission de réguler, sinon les activités spatiales elles-mêmes, du moins leurs applications et produits dérivés sous le couvert de son omnipotence en matière de marché intérieur. C'est un signal fort que certains Etats n'ont pas dû apprécier. Le marché de l'observation de la Terre reste un domaine commercial sensible où l'intervention étatique constitue une donnée fondamentale (que ce soit au travers des programmes de développement de technologie satellitaire ou des achats de données pour les besoins institutionnels). La part d'autorité traditionnellement réservée à la Commission est celle qui porte sur ses propres activités, en l'espèce celles de son programme Copernicus dont elle fixe elle-même les modalités et conditions d'accès aux données.

La Commission avait indiqué son intention de revenir avec une nouvelle proposition de directive en 2016, ce qui n'a pas été le cas. Cet échec de la proposition européenne est regrettable dans la mesure où il laisse les Etats membres en ordre dispersé face aux géants du Net actifs dans le domaine de la

[18] A noter l'exclusion implicite des relations internationales des entités fédérées.

cartographie et face à la communauté internationale au sein de laquelle certaines puissances n'hésitent pas à recourir à la censure ou à la corruption des données afin de protéger leurs intérêts stratégiques.

(iii) Le Code pénal (Livre II, Titre premier, Chapitre II)

L'annonce d'une plainte contre Google fin septembre 2018 par le Ministre Vandeput n'a pris personne au dépourvu, et certainement pas Google. Cette dernière a d'ailleurs communiqué en réplique en indiquant regretter la décision belge étant donné les pourparlers en cours depuis plus deux ans, pourparlers ayant abouti, selon Google, à « *des modifications (de) nos cartes où cela était demandé et où il existe un cadre légal en droit belge pour une telle demande* »[19].

Précisément, la question de l'état du droit belge en la matière fait l'objet de discussions qui remontent à 2008, Pieter De Crem alors Ministre de la Défense. A cette époque, les applications en ligne de Google sont déjà identifiées comme posant un « risque de sécurité » et justifient une demande du Gouvernement belge à Google Inc. de brouiller les images des cantonnements de l'armée belge en opération à l'étranger. Une liste de 146 sites sur le territoire belge a en outre été communiquée à Google afin que les images correspondantes se voient limiter à une résolution supérieure ou égale à 50 cm. Cette limite était d'ailleurs annoncée par le Ministre comme le seuil applicable à la transposition de la Directive UE « INSPIRE » afin de protéger la vie privée. Elle correspond en outre à la limite imposée par le Gouvernement américain à ses opérateurs satellitaires[20].

Simultanément, le Ministre de la Défense, également en charge de l'Institut Géographique National (IGN), avait mis sur pied un groupe de travail interdépartemental regroupant ses collaborateurs, ceux du département de la Justice et ceux du département de l'Intérieur, avec pour mission de réfléchir à un cadre légal approprié visant à assurer la protection des sites sensibles sur le territoire belge en limitant la diffusion publique d'images et de données géographiques les concernant. La première phase de cette réflexion avait porté sur une possible révision de l'article 120ter du Code pénal. Dans une seconde phase dès fin 2009, le groupe de travail s'était élargi à d'autres départements (Politique scientifique fédérale et IGN) afin d'intégrer ces préoccupations dans un exercice plus large incluant la transposition de la Directive INSPIRE précitée.

L'initiative du Ministre De Crem fera néanmoins long feu, du moins en ce qui concerne la révision du Code pénal. Mais la réflexion permettra de mettre en exergue la difficulté de réguler la publication en ligne, par des sociétés étrangères, de données relatives au territoire belge ou aux opérations militaires belges à l'étranger. Qui plus est, l'origine satellitaire de certaines de ces données rend l'analyse juridique d'autant plus complexe que leur captation originelle échappe à l'empire de la loi belge. Toujours est-il qu'un avant-projet de loi révisant l'article 120ter du Code pénal fut préparé par le groupe de travail. Son objectif était de supprimer toute ambigüité quant au champ d'application de cette disposition en incluant explicitement les données « d'origine aérienne ».

L'article 120ter du Code pénal se lit comme suit :

> « *Sera puni d'un emprisonnement de huit jours à un an et d'une amende de 26 à 100 euros :*
>
> *1° Quiconque, sans autorisation de l'autorité militaire, maritime ou aéronautique, aura exécuté par un procédé quelconque des levés ou opérations de topographie dans un rayon d'un myriamètre ou dans tout autre rayon qui sera ultérieurement fixé par le Ministre de la défense nationale, autour d'une place forte, d'un ouvrage de défense, d'un poste, d'un établissement militaire ou maritime, d'un établissement aéronautique autre qu'un aérodrome*

[19] Cf. LeSoir.be, 28/09/2018.
[20] Cf. plus haut, note de bas de page n°14.

ou aérogare, d'un dépôt, magasin ou parc militaires, à partir des ouvrages avancés, ou aura pris des photographies d'un de ces lieux, ouvrages ou établissements, édité, exposé, vendu ou distribué des reproductions de ces vues;

2° Quiconque, sans autorisation, aura escaladé ou franchi soit les revêtements ou les talus des fortifications, soit les murs, barrières, grilles, palissades, haies ou autres clôtures, établis sur un terrain militaire ou aura pénétré dans un fort ou l'un des autres établissements visés par l'article 120bis, 1°. »

L'avant-projet de loi proposé par le groupe de travail en 2010 le révisait ainsi (nous soulignons) :

« *Sera puni d'un emprisonnement de huit jours à un an et d'une amende de 26 à 100 euros :*

1° Quiconque, sans autorisation de l'autorité militaire, maritime ou aéronautique, aura exécuté par un procédé quelconque des levés ou opérations de topographie dans un rayon d'un myriamètre ou dans tout autre rayon qui sera ultérieurement fixé par le Ministre de la défense nationale, autour d'une place forte, d'un ouvrage de défense, d'un poste, d'un établissement militaire ou maritime, d'un établissement aéronautique autre qu'un aérodrome ou aérogare, d'un dépôt, magasin ou parc militaires, à partir des ouvrages avancés, ou aura pris ***, à partir d'un point situé sur le sol ou dans les airs,*** *des photographies d'un de ces lieux, ouvrages ou établissements, édité, exposé, vendu ou distribué des reproductions de ces vues;*

1°bis Quiconque, sans autorisation préalable de l'autorité militaire, aura édité, exposé, vendu ou distribué des vues satellitaires d'un établissement militaire visé au 1°, ou d'un campement militaire belge situé hors du territoire national ;

2° Quiconque, sans autorisation, aura escaladé ou franchi soit les revêtements ou les talus des fortifications, soit les murs, barrières, grilles, palissades, haies ou autres clôtures, établis sur un terrain militaire ou aura pénétré dans un fort ou l'un des autres établissements visés par l'article 120bis, 1°. »

On pourra commenter à souhait ces insertions, leur pertinence et leur applicabilité pratique. Toujours est-il que cet avant-projet de loi s'est égaré dans les limbes et les méandres des atermoiements politiques, alors que l'exécutif fédéral s'apprêtait à vivre sa plus longue crise de gestation.

La question reste donc de savoir si les dispositions du Code pénal inchangées sont susceptibles de s'appliquer au cas Google (toute question de compétence juridictionnelle mise à part). La réponse nous semble affirmative, car les ajouts proposés en 2010 tenaient à quelques précisions superfétatoires destinées à garantir l'application de la loi au cas spécifique des données Google. L'expression « *dans les airs* » était d'ailleurs ambigüe au regard de la nature physique de l'espace extra-atmosphérique. Quant à la première partie du nouveau point 1°bis tel que suggéré, on voit mal sa valeur ajoutée étant donné que l'édition, l'exposition, la vente et la distribution des images visées étaient déjà couvertes par le point 1°. La seule véritable nouveauté proposée en 2010 était l'inclusion des campements de campagne, c'est-à-dire des camps d'opération à l'étranger. Or, le texte n'explicitait pas comment cette disposition de droit belge allait s'appliquer, par exemple, à la diffusion, par l'Etat observé ou par un Etat tiers, de vues du territoire sur lequel les troupes belges étaient en mission. Si l'on songe à des opérations militaires dans le cadre de secours ou de gestion de catastrophes naturelles, il est vraisemblable que la zone sinistrée aurait été couverte à de multiples reprises et les données résultantes distribuées aux autorités et aux services d'intervention avant même que le commandement militaire belge eût pu donner son autorisation.

Il est à noter que l'infraction érigée à l'article 120ter, 1°, du Code pénal ne requiert pas la démonstration d'un élément intentionnel spécifique. Contrairement à d'autres infractions définies sous le même chapitre, la prise de vues, leur édition, leur exposition, leur vente et leur distribution sont punissables alors même que l'auteur n'avait pas connaissance de l'objet représenté. En Belgique, les « places fortes », ouvrages de défense, postes ou établissements aéronautiques et autres dépôts, magasins ou parcs militaires ne sont pas légion, encore qu'ils ne soient pas nécessairement évidents à identifier ou à localiser. Sur d'autres territoires, de telles installations sont tenues secrètes et situées dans des zones isolées, à tel point que le jeu consiste à les repérer sur Google Earth. Ceci implique la difficulté, du moins pour certains sites et pour certaines installations, d'être relevés comme tels par l'éditeur de données, à moins de se référer à une liste officielle arrêtée par les autorités compétentes. En l'absence d'une telle liste, il appartient auxdites autorités d'informer l'éditeur des sites et installations tombant dans le champ de l'article 120ter, 1°, du Code pénal. C'est la démarche qui a été entreprise par le Ministre belge de la Défense auprès de Google. Une telle démarche peut, dans certains cas, poser problème lorsque la localisation, l'existence ou l'affectation du site ou de l'installation est elle-même une information classifiée. Un autre problème posé par une liste établie a posteriori hors de tout contrôle parlementaire est le respect du droit à l'information : rien n'empêche l'autorité – militaire ou autre – d'inclure dans la liste certains sites dont l'exposition publique pourrait avoir un impact politique indésirable (ex. : camps de réfugiés).

La notion de « site sensible » que nous avons utilisée jusqu'à présent couvre en réalité plusieurs types de sites ou d'installations. Il peut d'abord s'agir de sites ou d'installations dont la représentation topographique, cartographique ou photographique constitue une information classifiée au sens de la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité. Cette loi prévoit la possibilité de protéger certaines informations (sous quelque forme que ce soit) ayant trait à la défense du territoire (y compris les plans de défense militaire), à la sûreté intérieure de l'Etat (y compris dans le domaine nucléaire) et aux relations internationales de la Belgique, au potentiel scientifique et économique du pays, à la sécurité des ressortissants belges à l'étranger (dont les militaires en opération), au fonctionnement des institutions ou à tout autre intérêt fondamental de l'Etat. Rappelons que le système de la protection par classification repose sur l'obligation imposée aux personnes habilitées d'éviter toute divulgation ou compromission des informations concernées. Il ne s'agit donc pas d'une obligation imposée de manière générale à tout citoyen. Il faut donc distinguer la divulgation du plan classifié d'un site militaire de la prise de vue aérienne (ou spatiale) du même site telle que visée par l'article 120ter, 1°, du Code pénal. A noter que le domaine nucléaire dispose de son propre système de classification aux termes de l'arrêté royal du 17 octobre 2011 portant sur la catégorisation et la protection des documents nucléaires.

Les infrastructures critiques sont un autre type de sites considérés comme sensibles. Elles font l'objet d'une loi du 1er juillet 2011 qui transpose la Directive 2008/114/CE du Conseil du 8 décembre 2008. La loi définit l'infrastructure critique comme « *toute installation, système ou partie [de système], d'intérêt fédéral, qui est indispensable au maintien des fonctions vitales de la société, de la santé, de la sûreté, de la sécurité et du bien-être économique ou social des citoyens, et dont l'interruption du fonctionnement ou la destruction aurait une incidence significative du fait de la défaillance de ces fonctions* ». Les infrastructures critiques sont de deux sortes : nationale, lorsque l'impact de leur dysfonctionnement se limite au territoire du pays où elles sont situées ; européenne, lorsque cet impact s'étend à au moins deux Etats membres de l'Union. A ce jour, la loi énumère quatre secteurs dans lesquels peuvent être identifiées des infrastructures critiques : les transports, l'énergie, les finances et les communications électroniques. Le Roi peut ajouter à cette liste d'autres secteurs en tant que de besoin. La protection desdites infrastructures s'articule en deux volets : les mesures internes et les mesures externes. Au titre de ces dernières, la Direction générale du Centre de crise du Service

public fédéral Intérieur (DGCC) peut prendre « *des mesures externes de protection des infrastructures critiques sur la base d'une analyse de la menace réalisée à sa demande ou d'office par l'OCAM* » (Organisme de Coordination de l'Analyse de la Menace). Cette disposition a donc une portée très générale. Il n'est toutefois pas certain qu'en l'absence de disposition légale explicite, elle permette à la DGCC d'interdire la diffusion de données satellitaires portant sur les infrastructures protégées. Il est déjà remarquable que le législateur ait habilité la DGCC, en lieu et place du Roi, à prendre de telles mesures. Ceci se justifie sans doute par la nécessité d'une approche au cas par cas en fonction de l'infrastructure, du contexte et des circonstances. On peut néanmoins se demander s'il n'appartient pas au Roi (et par Lui, au Ministre de l'Intérieur) de fixer le cadre dans lequel les mesures peuvent être prises par la DGCC.

(c) Droit étranger

Plusieurs pays ont adopté un cadre légal interne pour réguler la diffusion et la publication des données satellitaires d'observation de la Terre.

Les Etats-Unis n'ont évidemment pas attendu Google, ni Internet, pour encadrer l'opération de satellites d'observation de la Terre et l'accès aux données brutes (« *unenhanced data* »). Le *Land Remote-Sensing Policy Act* de 1992 a remplacé le *Land Remote-Sensing Commercialization Act* de 1984 et intègre à de nombreux endroits la notion de « *national security* » afin de tempérer le principe de libre accès ou de libre diffusion.

La France et l'Allemagne ont, quant à elles, adopté respectivement en 2008 et en 2010 une législation relative à la diffusion des données d'observation de la Terre par satellite[21]. Le principe de base de ces deux législations avait été largement repris par la Commission dans sa proposition de directive de 2014 (cf. ci-dessus) : en gros, les données sont soumises à un test de sensibilité et, le cas échéant, à un régime de permis limitant leur utilisation.

D'autres Etats ont, à des degrés divers, adopté des instruments juridiques ou/et politiques encadrant la diffusion des données satellitaires d'observation de la Terre (Royaume-Uni, Canada, Inde, Japon et Russie).

A l'échelle internationale, bien que l'idée d'un traité multilatéral régissant les activités d'observation de la Terre demeure le fantasme de certains Etats (en particulier des Etats en développement), aucun projet n'a été entrepris en ce sens au sein de l'UNCOPUOS. Des initiatives ont donné lieu à la mise sur pied de structures de coopération, telles que le GEO (Groupe intergouvernemental pour l'Observation de la Terre), mais aucun instrument liant ne régit le marché des données d'origine spatiale. Le seul essai transformé dans ce domaine est la Convention sur le Transfert et l'Utilisation des Données de Télédétection de la Terre depuis l'Espace extra-atmosphérique, faite à Moscou, le 19 mai 1978. En réalité, ce traité ne concerne que des pays alors ressortissant au Bloc soviétique[22]. La convention organise un partage des données satellitaires dans le respect des ressources naturelles et des intérêts nationaux respectifs. Si cette convention n'a pas été formellement dénoncée depuis l'éclatement de l'Union soviétique, il y a fort à parier qu'elle est depuis tombée en désuétude au vu du nouvel ordre régional.

[21] Loi n° 2008-518 du 3 juin 2008 relative aux opérations spatiales (titre VII) et *Satellitendatensicherheitsgesetz*, du 23 mars 2010.
[22] Cuba, Tchécoslovaquie, Allemagne de l'Est, Hongrie, Mongolie, Pologne, Roumanie et URSS.

En l'absence de traité multilatéral, la seule référence juridique commune reste la Résolution de l'Assemblée Générale des Nations Unies sur les Principes sur la Télédétection (41/65), du 3 décembre 1986.

Conclusion

Le développement impressionnant des technologies et applications satellitaires combiné à celui de la société de l'information multiplie quasiment à l'infini les possibilités d'utilisation, notamment sous la forme de produits commerciaux, des données géospatiales. On est enclin à penser que si une intervention législative était nécessaire pour garder la maîtrise de l'information ainsi diffusée, elle aurait dû avoir lieu il y a déjà longtemps. La duplication des données reprises sous des formats variés à travers l'ensemble de la Toile rend illusoire une censure a posteriori.

La solution la plus réaliste pour un Etat confronté à l'exposition de ses sites sensibles aux yeux du monde reste sans doute la négociation. Dans cette optique, la menace de sanctions pénales est un élément de pression plus ou moins crédible, *selon que vous soyez puissant ou misérable…*

Reste l'idée d'une censure a priori qui consiste à brider les capacités d'observations satellitaires dès leur entrée en opération. Là encore, eu égard aux principes du droit international et, plus spécifiquement des traités relatifs à l'espace extra-atmosphérique, la conciliation apparaît incontournable : seul l'Etat exerçant sa juridiction sur la mission satellitaire jouit de cette prérogative. C'est par le biais de l'autorisation octroyée à l'opérateur et par celui de la juridiction exercée sur le satellite que le contrôle gouvernemental sur la précision des données fournies peut se réaliser. Des accords internationaux pourraient théoriquement permettre aux gouvernements de s'accorder sur un niveau de résolution maximum pour les données satellitaires en fonction de leur usage. Mais il semble d'ores et déjà acquis que de telles restrictions conventionnelles ne toucheront pas les systèmes militaires. En outre, le marché commercial de l'observation de la Terre mise l'essentiel de son avenir sur la haute définition. Les obstacles intergouvernementaux à cette expansion se heurteraient très vraisemblablement à une vive contestation de la part du secteur. Et rien ne garantit que de tels accords empêcheraient la captation et la diffusion de données par les concurrents établis dans des Etats aux intérêts nationaux « divergents ».

L'aboutissement, quel qu'il soit, de l'action du Ministre de la Défense actuel ou de son successeur sera donc un événement significatif à analyser de près.

*