ASSEMBLÉE NATIONALE

17ème législature

Utilisation par l'État et les collectivités de logiciels de surveillance

Question écrite n° 1355

Texte de la question

M. Ugo Bernalicis interroge M. le ministre de l'intérieur sur l'utilisation par son ministère de logiciels de surveillance de l'entreprise Briefcam comprenant des dispositifs de vidéosurveillance algorithmique (VSA) et de reconnaissance faciale. Dans un article publié le 14 novembre 2023, le média d'investigation *Disclose* révèle que depuis des années, en se sachant dans l'illégalité la plus totale, la police nationale, la gendarmerie nationale et certaines polices municipales ont recouru au logiciel de l'entreprise Briefcam, qui permet d'automatiser l'analyse des images de vidéosurveillance algorithmiques et qui comporte une option « reconnaissance faciale » qui serait, d'après *Disclose*, « activement utilisée ». Précisément, d'après le média Disclose, la direction départementale de sécurité publique de Seine-et-Marne a été la première à expérimenter les technologies de l'entreprise Briefcam, avant d'être suivie par le Rhône, le Nord, les Alpes-Maritimes, la Haute-Garonne puis le service interministériel d'assistance technique (SIAT) et enfin les services de la police judiciaire, les préfectures de police de Paris et Marseille, la sûreté publique et la gendarmerie nationale. La vidéosurveillance automatisée est aujourd'hui interdite par le cadre de protection des données personnelles prévues par le règlement général sur la protection des données (RGPD) et la loi « informatique et libertés ». Son usage peut même être sanctionné aux termes des articles 226-18 et 226-19 du code pénal, selon lesquels « le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende ». L'usage en dehors de tout cadre légal et de tout contrôle d'un tel logiciel d'analyse d'images automatisées de reconnaissance faciale porte une atteinte grave et manifeste aux libertés fondamentales des personnes filmées. Le dispositif, par son caractère particulièrement intrusif, met directement en cause le droit au respect de la vie privée et des données personnelles pourtant protégé. En effet, l'enregistrement d'images, mis en relation de manière automatisée avec d'autres traitements de données à caractère personnel, permet la manipulation de données sensibles par les services de l'État et des collectivités territoriales en toute impunité. La dangereuse généralisation non maîtrisée de ces nouveaux dispositifs technologiques développe une surveillance généralisée susceptible de se répercuter sur les comportements des personnes, entravant leurs droits civils et politiques, comme leurs libertés d'aller et venir. C'est par ailleurs ce que la Commission nationale de l'informatique et des libertés (CNIL) a indiqué, dans son avis de juillet 2022 : la « généralisation non maîtrisée de ces dispositifs [de VSA], par nature intrusifs, conduirait à un risque de surveillance et d'analyse généralisée dans l'espace public ». Cette révélation est particulièrement inquiétante, compte tenu du caractère attentatoire au droit fondamental à la vie privée et dans la perspective des jeux Olympiques de 2024, alors même que l'interdiction de systèmes automatisés de reconnaissance faciale était présentée comme une garantie (de la légalisation de la vidéosurveillance algorithmique) lors de la loi relative aux jeux Olympiques du 19 mai 2023. Alors que de fortes présomptions existaient depuis plusieurs années quant à son utilisation par la police nationale, cette révélation d'un usage de la vidéosurveillance algorithmique (VSA) est gravissime tout autant pour son caractère illégal, qu'en raison des dissimulations et détournements dont ce marché public hautement sensible a fait l'objet de la part de hauts fonctionnaires et de responsables politiques. L'impuissance chronique à laquelle se condamnent les contre-pouvoirs institutionnels, de la Commission nationale de l'informatique et des libertés (CNIL) à l'inspection générale de la police nationale (IGPN), est symptomatique d'une crise systémique de l'État de droit. Au vu de cet exposé et en raison de l'ensemble des questions soulevées par ce grand chantier, il souhaiterait savoir comment ce déploiement de

logiciels de surveillance de l'entreprise Briefcam a été mis en place au sein des services de l'État ; à partir de quand et de quelle manière a été associée la Commission nationale de l'informatique et des libertés à cette utilisation des solutions de Briefcam ; comment ces logiciels de surveillance de l'entreprise Briefcam sont actuellement structurés, notamment en prévision des jeux Olympiques ; combien de communes en France et en Île-de-France sont concernées par le déploiement de systèmes de VSA et, le cas échéant, lesquelles le sont et dans quelle mesure le grand public, les élus locaux et les habitants en ont, ou non, été informés.

Texte de la réponse

Les fichiers de police sont des outils de travail indispensables pour les forces de sécurité intérieure et le ministre d'Etat, ministre de l'Intérieur est déterminé à ce qu'elles disposent des moyens, notamment technologiques, les plus performants pour exercer leurs missions. Ces fichiers représentent également, à l'instar de diverses technologies déployées par des acteurs privés, d'importants enjeux en matière de garanties des libertés publiques. Tout fichier de police doit répondre à des exigences juridiques fortes, tant pour sa création que pour son utilisation. Les fichiers mobilisent des données dont le caractère personnel oblige à se conformer notamment à la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés et au « paquet européen de protection des données à caractère personnel » (règlement du 27 avril 2016 dit règlement général sur la protection des données et directive du 27 avril 2016 dite directive police-justice). Le respect de ce cadre juridique est soumis au contrôle de la Commission nationale de l'informatique et des libertés. S'agissant du traitement « Vidéo Synopsis » (dit BriefCam), il s'agit d'un logiciel d'analyse vidéo utilisé par les services de police et les unités de gendarmerie pour simplifier et accélérer le travail des enquêteurs. Il ne peut être utilisé que dans un cadre judiciaire, en temps différé, et non en police administrative, en temps réel. Ainsi, les décisions d'acquisition du logiciel BriefCam résultaient du besoin d'exploiter à des fins judiciaires une masse considérable d'images vidéo, de réduire le temps nécessaire à leur visionnage par le recours à un outil numérique de « dérushage » et de rationaliser le travail des enquêteurs en privilégiant d'autres activités à plus forte valeur ajoutée. En gendarmerie, ce logiciel a une vocation de traitement de la criminalité du haut du spectre plutôt que de la délinquance du quotidien. Sur le plan juridique, il correspond à un logiciel de rapprochement judiciaire. Le régime juridique des logiciels de rapprochement judiciaire, défini à l'article 230-20 du code de procédure pénale, dispose que ces derniers ont pour finalité de « faciliter le rassemblement des preuves des infractions et l'identification de leurs auteurs » ainsi que « l'exploitation et le rapprochement d'informations sur les modes opératoires réunies au cours des enquêtes ou procédures dont les services de police et de gendarmerie nationales ont la charge ». Il convient à cet égard de rappeler que le décret n° 2012-687 du 7 mai 2012 relatif aux traitements automatisés de données à caractère personnel dénommé « logiciel de rapprochement judiciaire à des fins d'analyse criminel » autorise la mise en œuvre des traitements de données à caractère personnel après envoi à la Commission nationale de l'informatique et des libertés d'un engagement de conformité. Dans un premier temps, le logiciel Briefcam, dont l'acquisition sporadique par les forces de l'ordre est d'ailleurs intervenue dans une période marquée par l'évolution du droit relatif aux données, n'a pas été considéré par ses utilisateurs comme pouvant avoir un statut spécifique dans la procédure, dans la mesure où il ne produit aucune pièce ni documentation directement intégrée à la procédure. En outre, ce logiciel n'est installé que sur un ordinateur dédié, déconnecté de toute base de données. Briefcam n'a donc pas été initialement considéré par les services enquêteurs comme un LRJ au sens du décret n° 2012-687 du 7 mai 2012. Dans sa position sur les conditions de déploiement des caméras dites « intelligentes » ou « augmentées » dans les espaces publics, publiée en juillet 2022, la CNIL ne considère pas que ces technologies sont, par principe, interdites par le RGPD et la loi dite « informatique et libertés ». Elle précise uniquement : « Sauf à ce que l'utilisation de tels dispositifs puisse s'inscrire dans les prérogatives de police judiciaire déjà prévues par le code de procédure pénale (pouvoirs généraux d'enquête du procureur de la République et du juge d'instruction), le recours à des analyses algorithmiques d'images de caméras de vidéoprotection, réalisées en temps réel en vue d'une intervention immédiate ou de l'enclenchement de procédures administratives ou judiciaires par les services de police, semble devoir être subordonné à l'existence d'un encadrement législatif spécifique. ». La position de la CNIL a été suivie par le législateur, dans la mesure où l'article 10 de la loi n° 2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions a institué, à titre expérimental, un cadre permettant d'appliquer aux images collectées au moyen de systèmes de

vidéoprotection ou de caméras installées sur des aéronefs des traitements algorithmiques à la seule fin d'assurer la sécurité des manifestations sportives, récréatives ou culturelles qui, par l'ampleur de leur fréquentation ou par leurs circonstances, sont particulièrement exposées à des risques d'actes de terrorisme ou d'atteintes graves à la sécurité des personnes. Préalablement à l'expérimentation prévue par la loi du 19 mai 2023 précitée, qui poursuit une finalité de police administrative, le législateur avait autorisé le recours à des logiciels d'aide aux enquêtes judiciaires. En particulier, les articles 230-20 à 230-27 du code de procédure pénale permettent aux services de la police nationale et aux unités de la gendarmerie nationale chargés d'une mission de police judiciaire de mettre en œuvre, sous le contrôle de l'autorité judiciaire, des logiciels destinés à faciliter l'exploitation et le rapprochement d'informations sur les modes opératoires réunies par ces services et unités au cours des procédures judiciaires. Dans le sillage de l'article de presse relatif à l'utilisation du logiciel BriefCam, le ministre de l'intérieur a diligenté une enquête administrative menée conjointement par l'inspection générale de l'administration, l'inspection générale de la police nationale et l'inspection générale de la gendarmerie nationale afin de déterminer les conditions dans lesquelles ces usages ont eu lieu et de s'assurer de leur conformité au cadre légal. De plus, ses services apportent en parallèle leur concours à un contrôle initié par la CNIL. Depuis, conformément au droit applicable, la direction générale de la police nationale a transmis à la Commission nationale de l'informatique et des libertés le 14 décembre 2023 un engagement de conformité attestant mettre en œuvre ce logiciel comportant des données à caractère personnel dans le respect des dispositions législatives et réglementaires applicables. La Commission nationale de l'informatique et des libertés a accusé réception de cet engagement le 15 décembre 2023. Par ce récépissé, l'utilisation du logiciel dit BriefCam répond aux exigences posées par le cadre juridique en vigueur. La direction générale de la gendarmerie nationale a quant à elle suspendu l'utilisation du logiciel BriefCam à compter du 17 novembre 2023 et a procédé à la désinstallation des suites logicielles en attendant une consolidation du cadre juridique. Conformément aux conclusions de l'enquête administrative, présentées dans un rapport remis au ministre de l'intérieur le 15 février 2024 et publié sur le site du ministère, la direction générale de la gendarmerie nationale a procédé à une régularisation de ce traitement de données auprès de la CNIL par l'envoi d'un engagement de conformité le 7 octobre 2024 et la CNIL en a accusé réception le lendemain. Pour autant, la gendarmerie nationale n'a pas redéployé pour l'instant le logiciel BriefCam au profit de ses unités de police judiciaire. Le traitement réalisé par BriefCam est actuellement utilisé dans un nombre restreint de services judiciaires de la police nationale et son usage répond à des critères strictement définis. Seul un nombre limité d'agents de la police nationale qui sont individuellement désignés et habilités ont accès au traitement. Les accédants sont donc restrictivement limités. Une procédure analogue est envisagée pour la gendarmerie nationale si le logiciel venait à être réinstallé sur des postes informatiques en vue d'une reprise de son utilisation après le rachat de licences. Concernant la collecte et le stockage des données révélées par l'exploitation des enquêtes, ces dernières sont effacées à la clôture de l'enquête et, en tout état de cause, à l'expiration d'un délai de trois ans à compter de leur enregistrement, conformément à la décision du Conseil constitutionnel du 10 mars 2011. Par ailleurs, ces outils ne peuvent analyser que des images ayant été obtenues dans le cadre exclusif d'une enquête judiciaire, avec l'ensemble des garanties que ce cadre judiciaire implique. Ils ne sont donc pas utilisés pour réaliser des analyses de l'image en temps réel. En outre, aucune « décision automatique » n'est prise par l'outil, qui n'est qu'une aide à l'enquête, toute décision étant prise par l'enquêteur. De plus, ces logiciels ne sont interconnectés avec aucun autre traitement. Plusieurs autres mesures contribuent à la sécurité de l'intégrité des données. Les données d'une enquête sont accessibles exclusivement aux personnes autorisées dans le cadre de ladite enquête. Vidéo Synopsis ne permet aucun partage des données, ce qui maximise la protection de celles-ci. Le traitement est accessible uniquement aux utilisateurs de l'application, identifiés et habilités sur un ordinateur dédié, qui n'est pas connecté à internet. Aussi et conformément aux dispositions du code de procédure pénale applicables en la matière, aucun dispositif de reconnaissance faciale ne peut être mis en œuvre. Cette nécessité a d'ailleurs été rappelée par instruction du directeur général du 6 février 2023 adressée à l'ensemble des services utilisateurs. Dans ce cadre, le logiciel n'a pas été acheté ni déployé dans l'intention de mettre en œuvre de la reconnaissance faciale puisque cette fonctionnalité n'existait pas lors des acquisitions initiales. Désormais, le fabricant s'est engagé à bloquer nativement le module qui permettrait d'accéder à des fonctionnalités de reconnaissance faciale pour la version française du logiciel. Le ministère de l'intérieur garantit ainsi la protection des données à caractère personnel collectées par le logiciel BriefCam. Dans un souci de transparence, il a également rendu public le 28 octobre 2024, sur le site internet du ministère (interieur.gouv.fr/publications/rapports de l'inspection générale de l'administration) un rapport inter-inspections

relatif à l'usage de logiciels d'analyse vidéo par les services de la police et de la gendarmerie nationales, commandé précisément en réponse à la dénonciation par un organisme spécialisé - cité dans la question écrite - d'une utilisation prétendument illégale par la police nationale, depuis 2015, d'un logiciel d'analyse algorithmique d'images vidéo qui utiliserait la reconnaissance faciale. Ce rapport contient des préconisations à la mise en œuvre desquelles les services du ministère travaillent.

Données clés

Auteur : M. Ugo Bernalicis
Circonscription : Nord (2e circonscription) - La France insoumise - Nouveau Front Populaire
Type de question : Question écrite
Numéro de la question : 1355
Rubrique : Sécurité des biens et des personnes
Ministère interrogé : Intérieur
Ministère attributaire : Intérieur

Date(s) clée(s)

Date de signalement : Question signalée au Gouvernement le 31 mars 2025
Question publiée au JO le : 22 octobre 2024, page 5582
Réponse publiée au JO le : 3 juin 2025, page 4467