ASSEMBLÉE NATIONALE

16ème legislature

Question N° : 13745	De **M. Ugo Bernalicis** (La France insoumise - Nouvelle Union Populaire écologique et sociale - Nord)	**Question écrite**

Ministère interrogé > Intérieur et outre-mer	**Ministère attributaire** > Intérieur et outre-mer

Rubrique >sécurité des biens et des personnes	**Tête d'analyse** >Utilisation par l'Etat et les collectivités de logiciels de surveillance	**Analyse** > Utilisation par l'Etat et les collectivités de logiciels de surveillance.

Question publiée au JO le : **12/12/2023**
Date de changement d'attribution : **12/01/2024**
Date de renouvellement : **16/04/2024**
Question retirée le : **11/06/2024** (fin de mandat)

Texte de la question

M. Ugo Bernalicis interroge M. le ministre de l'intérieur et des outre-mer 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.