ASSEMBLÉE NATIONALE

14ème legislature

Question N° : 42308	De **M. Guillaume Larrivé** (Union pour un Mouvement Populaire - Yonne)	**Question écrite**

Ministère interrogé > Intérieur	**Ministère attributaire** > Intérieur

Rubrique >police	**Tête d'analyse** >police nationale	**Analyse** > police 3-0. orientations.

Question publiée au JO le : **12/11/2013**
Réponse publiée au JO le : **22/07/2014** page : **6239**
Date de changement d'attribution : **03/04/2014**
Date de renouvellement : **29/04/2014**

Texte de la question

M. Guillaume Larrivé interroge M. le ministre de l'intérieur sur le concept de "police 3-0" qu'il a mentionné lors de récents discours. Il le remercie de bien vouloir préciser les objectifs, les moyens, la doctrine d'emploi ainsi que, le cas échéant, le calendrier de déploiement de la "police 3-0".

Texte de la réponse

Pour répondre aux nouvelles exigences de la population, continuer à s'adapter aux nouvelles formes de délinquance sur Internet, à les prévenir et à les anticiper, les forces de police et de gendarmerie doivent être pleinement intégrées dans l'espace numérique. Depuis plusieurs années déjà, le ministère de l'intérieur s'est engagé dans cette voie, par exemple dans la lutte contre la cybercriminalité avec la plateforme de signalement des contenus illicites (www. internet-signalement. gouv. fr) ou avec la diffusion d'informations sur des malfaiteurs présumés recherchés ou sur des objets volés (www. avisderecherches. interieur. gouv. fr). Face à l'augmentation des cybermenaces, il est cependant indispensable de « monter en gamme ». Le ministre de l'intérieur a ainsi demandé, début 2014, aux directeurs généraux de la police et de la gendarmerie nationales de définir un plan d'action ministériel permettant de gagner en efficacité et en réactivité. Le rapport sur la lutte contre les cybermenaces en matière de sécurité intérieure lui a été remis le 31 mai. Il propose six axes stratégiques d'action (renforcer le niveau de sécurité des systèmes d'information, promouvoir la coopération internationale, améliorer le niveau de sensibilisation et de prévention des particuliers, des acteurs économiques et des collectivités territoriales, etc.). Ces préconisations ont été validées et un délégué ministériel à la lutte contre les cybermenaces sera nommé à bref délai. D'ores et déjà, la création d'une sous-direction dédiée à la lutte contre la cybercriminalité au sein de la direction centrale de la police judiciaire va permettre de renforcer les capacités de réponse du ministère de l'intérieur. Le ministère de l'intérieur prend également pleinement en compte les enjeux numériques de la lutte contre le terrorisme. Dans le cadre du plan de lutte contre la radicalisation violente et les filières terroristes présenté en conseil des ministres le 23 avril, qui prévoit plusieurs adaptations législatives prochainement soumises au Parlement, les possibilités de détection des filières sur Internet seront accrues et les outils de lutte contre le cyber-terrorisme étoffés. Des impulsions seront également données, en France comme au niveau européen, en direction des grands opérateurs d'Internet, afin que les contenus illicites (images, vidéos...) et les sites de recrutement fassent l'objet de procédures de suppression effectives et rapides. La rencontre, co-présidée par la France et la Belgique, qui s'est tenue le 8 mai 2014 à Bruxelles puis le 5 juin 2014 à Luxembourg entre les neuf pays européens les plus concernés par le risque terroriste djihadiste a permis à cet égard de premières avancées. Dans une société de

réseaux marquée par les flux d'images, de données et d'informations en temps réel, dans un environnement où le développement des technologies et Internet favorisent la transparence mais aussi la surexposition, les forces de l'ordre doivent également être visibles et actives pour expliquer et valoriser leur action, pour agir et réagir aux événements avec efficacité. Les initiatives se sont ainsi développées pour moderniser et faciliter les démarches en ligne (lapolicerecrute. fr...), comme par exemple avec le téléservice de « pré-plainte en ligne » (www. pre-plainte-en-ligne. gouv. fr) généralisé depuis début 2013. De même, à l'occasion de la récente réforme de l'inspection générale de la police nationale destinée à en accroître la transparence et l'ouverture à la société, une plate-forme internet de recueil des signalements a été mise en place début septembre 2013, accessible à partir du site du ministère de l'intérieur (rubrique mes démarches/mes téléservices) et permettant à quiconque de signaler en ligne des manquements présumés à la déontologie dont il s'estimerait victime ou dont il serait témoin. Dès aujourd'hui il faut consolider et renforcer la police et la gendarmerie « web 2.0 ». La présence des forces de l'ordre sur Internet et sur les réseaux sociaux, en particulier, est déjà une réalité (Facebook, Twitter, DailyMotion...). Elle doit encore s'accentuer pour permettre une communication moderne. Ces initiatives vont se poursuivre, car dans ce domaine l'adaptation doit être constante. D'autres innovations sont donc à rechercher dans la communication et le contact avec la population, par exemple pour toucher de manière ciblée la diversité des publics (jeunes, commerçants, riverains d'un quartier, agriculteurs, alertes aux populations...). Au delà, il s'agit également d'intégrer les évolutions technologiques aux stratégies de sécurité pour en tirer tous les bénéfices. Pour bâtir une « police 3.0 », un groupe de travail police/gendarmerie/sécurité civile, associant également des experts extérieurs, a été mis en place à l'automne 2013. Dans les conclusions qu'il a récemment rendues, il propose un chiffrage et une programmation des projets technologiques pour le budget triennal 2015-2017. Les projets identifiés concernant les technologies actuelles ou émergentes qui s'inscrivent dans une stratégie à court terme (cinq prochaines années) et dans une démarche prospective à l'horizon 2025. Quatre enjeux stratégiques ont été identifiés : répondre à une société de plus en plus numérique par une proximité renouvelée (réseaux sociaux, unification des plates-formes de réception des appels d'urgence...) ; améliorer l'efficacité du primo-intervenant (réseaux de haut-débit pour les transmissions...) ; développer des capacités d'anticipation et de conduites opérationnelles (cartographie décisionnelle, analyse prédictive...) ; lutter contre la criminalité avec des moyens technologiques adaptés (nouvelle génération d'outils de police technique et scientifique...). Sur le plan organisationnel, le ministère de l'intérieur, qui disposait déjà d'un service des technologies et des systèmes d'information de la sécurité intérieure, commun à la police et à la gendarmerie, s'est récemment doté d'une mission de gouvernance ministérielle des systèmes d'information et de communication. Les fonctions d'information et de communication ont par ailleurs été modernisées et renforcées dans le cadre de la récente réforme de l'administration centrale.