JURISPRUDENCE

Cass. (2e ch. N), 13 décembre 2016[1]

Note d'observations de Elise Degrave[2]

PROTECTION DE LA VIE PRIVÉE ET DES DONNÉES À CARACTÈRE PERSONNEL – E-GOUVERNEMENT – POLICE – AMENDE

PRIVACY AND DATA PROTECTION – E-GOVERNMENT – POLICE – FINE

Dans l'arrêt commenté, la Cour de cassation met en évidence que les données à caractère personnel des citoyens, détenues par l'État, font l'objet d'une protection particulière. Un comité sectoriel de la Commission de la protection de la vie privée doit en effet en autoriser l'utilisation, jouant le rôle de « chien de garde » des données détenues par les administrations.

Si un policier ne respecte pas cette règle et identifie un contrevenant sans autorisation, l'amende infligée est-elle nulle ? C'est à cette question que répond la présente analyse, fondée sur l'étude des multiples règles applicables à ce cas d'espèce.

• • •

In the commented decision, the Court of cassation emphasizes the fact that personal data of citizens, held by the State, are subject to special protection. A sectorial committee of the Privacy Commission must indeed authorize its use, thus acting as a "watchdog" for data held by administrations.

If a police officer does not respect this rule and identifies an unauthorized offender, will the fine imposed on him be considered void? This is the leading question of the following analysis, based on the study of the various applicable rules to this case.

I. LA PROCÉDURE DEVANT LA COUR

Le pourvoi est dirigé contre un jugement rendu le 11 mai 2016 par le tribunal correctionnel néerlandophone de Bruxelles, statuant en degré d'appel.

Le demandeur fait valoir cinq moyens dans un mémoire annexé au présent arrêt, en copie certifiée conforme.

Le conseiller Alain Bloch a fait rapport.

L'avocat général délégué Alain Winants a conclu.

II. LA DÉCISION DE LA COUR

Sur le premier moyen

1. Le moyen invoque la violation de l'article 18 de la loi du 19 mai 2010 portant création de la Banque-Carrefour des véhicules (ci-après : loi du 19 mai 2010) : le jugement attaqué considère à tort que, lors de l'exécution des missions qui lui sont imparties conformément aux articles 8 du Code d'instruction criminelle, 1 et 15 de la loi du 5 août 1992 sur la fonction de police, 62 de la loi du 16 mars 1968 relative à la police de la circulation routière et 3 de l'arrêté royal du 1er décembre 1975 portant règlement général sur la police de la circulation routière, la police peut, pour identifier le titulaire d'une plaque d'immatriculation par le biais de la Direction pour l'immatriculation des véhicules, faire appel aux données reprises dans la Banque-Carrefour des véhicules sans disposer d'une autorisation du Comité sectoriel pour l'autorité fédérale de la Commission de protection de la vie privée (ci-après le Comité sectoriel) ; le jugement attaqué considère également à tort

que l'identification du titulaire de la plaque d'immatriculation d'un véhicule n'implique pas la divulgation de données à caractère personnel.

2. Conformément à l'article 8 de la loi du 19 mai 2010, le répertoire matricule des véhicules prévu aux articles 6, 7, 8 et 9 de l'arrêté royal du 20 juillet 2001 relatif à l'immatriculation de véhicules est tenu à jour par la Banque-Carrefour. Ce répertoire matricule mentionne notamment le numéro de la plaque d'immatriculation du véhicule et les données à caractère personnel concernant le titulaire du certificat d'immatriculation.

3. Suivant l'article 7, alinéas 1er et 2, de la loi du 19 mai 2010, les véhicules enregistrés sont identifiés par un numéro d'identification unique et l'enregistrement va de pair notamment avec l'indication des données mentionnées dans le certificat de conformité et des données d'identification de la personne physique ou morale propriétaire du véhicule.

4. L'article 2, 10°, de la loi du 19 mai 2010 définit une donnée à caractère personnel comme toute information concernant une personne physique identifiée ou identifiable.

5. Les données d'identification du propriétaire et du titulaire qui est une personne physique sont, tout comme le numéro de la plaque d'immatriculation, pareilles données à caractère personnel.

6. L'article 18, § 1er, de la loi du 19 mai 2010 dispose qu'une autorisation du Comité sectoriel est requise pour tout accès aux données de la Banque-Carrefour des véhicules autres que les données mentionnées dans le certificat de conformité du véhicule.

7. Le fait qu'il relève de la mission de la police de rechercher et constater les infractions de roulage n'entraîne pas que la police puisse, pour identifier le titulaire d'une plaque d'immatriculation par le biais de la Direction pour l'immatriculation des véhicules, avoir accès aux données personnelles de la Banque-Carrefour des véhicules sans l'autorisation du Comité sectoriel.

Le jugement attaqué qui rend une autre décision n'est pas légalement justifié.

Dans cette mesure, le moyen est fondé.

Sur les autres griefs

8. Il n'y a pas lieu de répondre aux autres griefs qui ne sauraient entraîner une cassation sans renvoi.

Par ces motifs,

La Cour

Casse le jugement attaqué ;

Ordonne que mention du présent arrêt sera faite en marge du jugement cassé ;

Réserve les dépens pour qu'il soit statué sur ceux-ci par le juge du fond ;

Renvoie la cause au tribunal correctionnel de Louvain, siégeant en degré d'appel.

Note d'observations[1]

PV pour excès de vitesse : les services de police peuvent-ils accéder librement aux données de la DIV ?

INTRODUCTION

Un conducteur commet un excès de vitesse, constaté par un dispositif de caméras. Pour lui faire parvenir le procès-verbal et la demande de paiement de l'amende, les services de police verbalisant doivent obtenir l'identité et l'adresse du titulaire de la plaque d'immatriculation concernée. Peuvent-ils, pour ce faire, consulter librement le répertoire matricule des véhicules de la DIV ?

Non. Comme le rappelle l'arrêt commenté[2], les données à caractère personnel des citoyens détenues par l'administration, telles que la plaque d'immatriculation et l'adresse du titulaire de celle-ci, font l'objet d'une protection particulière. Cette protection est exercée par les comités sectoriels, organes institués au sein de la Commission de la protection de la vie privée. Il en résulte que l'accès et l'utilisation de ces données sont soumis au respect de procédures spécifiques.

En l'espèce, même si l'utilisation des données à caractère personnel des citoyens entre dans les missions légales de la police[3], cette dernière doit obtenir l'autorisation du Comité sectoriel de l'autorité fédérale avant d'obtenir des données du répertoire matricule des véhicules par l'intermédiaire de la Banque-Carrefour des véhicules, à défaut de quoi, l'envoi du PV sera fondé sur une preuve irrégulière.

Après avoir situé le cas d'espèce dans le paysage de l'administration électronique belge, le présent commentaire fait le point sur le rôle des comités sectoriels de la Commission de la protection de la vie privée et la procédure d'accès aux données de la DIV.

I. LA BANQUE-CARREFOUR DES VÉHICULES (« BCV ») AU CŒUR D'UN RÉSEAU SECTORIEL

L'arrêt commenté évoque le rôle de la BCV comme intermédiaire dans la communication des données réclamées par la police. Le souci de clarté impose de contextualiser cette notion récente.

Depuis plusieurs années à présent, l'administration belge est engagée dans la voie de l'e-gouvernement, dit aussi « administration électronique ». Cette évolution se manifeste notamment par une réorganisation profonde de la collecte et de l'enregistrement des données à caractère personnel des citoyens dont l'État a besoin pour assurer ses missions. En somme, différents réseaux sectoriels sont créés au sein de l'administration, qui comprennent des administrations distinctes liées par une thématique commune. Parmi ces réseaux figure notamment le « réseau sectoriel de la Banque-Carrefour des véhicules », organisé par une loi du 19 mai 2010[4]. Ce réseau comprend différentes administrations qui

1 Elise Degrave. Chargée de cours à la Faculté de droit de l'UNamur (Crids).

2 Trois autres arrêts rendus par la Cour de cassation le 13 décembre 2016 vont dans le même sens (R.G. n^{os} P160723N, P160786N et P160909N).

3 Voy. l'article 44/1 de la loi du 5 août 1992 sur la fonction de police, *M.B.*, 22 décembre 1992 (ci-après « loi sur la fonction de police »).

4 Loi du 19 mai 2010 portant création d'une Banque-Carrefour des véhicules, *M.B.*, 28 juin 2010 (ci-après, « loi BCV »).

collectent et/ou utilisent des données relatives aux véhicules et aux titulaires des plaques d'immatriculation, notamment.

Les données ayant vocation à circuler au sein d'un réseau sectoriel sont enregistrées dans des « sources authentiques de données »[5], qui sont des bases de données particulièrement fiables placées sous la responsabilité d'une administration. Par exemple, le répertoire matricule des véhicules est une des sources authentiques de données du réseau sectoriel de la Banque-Carrefour des véhicules et est placé sous la responsabilité du SPF Mobilité et Transport[6].

Au cœur de ce réseau sectoriel se trouve la BCV, qu'évoque la Cour de cassation dans l'arrêt commenté. La BCV assure le rôle d'« intégrateur de services », chargé de faire circuler les données au sein du réseau sectoriel de la Banque-Carrefour des véhicules. Plus précisément, lorsqu'une administration a besoin d'une donnée « véhicule » dont elle ne dispose pas, elle contacte la BCV qui va la chercher dans la source authentique adéquate et l'achemine vers l'administration qui l'a demandée. La loi BCV détermine les finalités de la BCV, parmi lesquelles figure le fait, pour chaque véhicule, « d'identifier leur propriétaire, le demandeur et le titulaire de leur immatriculation », afin, notamment, de « faciliter la recherche, la poursuite pénale et l'application des peines des infractions »[7]. Les données qui ont vocation à circuler au sein de ce réseau ainsi que les services chargés de les collecter sont déterminés par arrêté royal[8].

II. LE CONTRÔLE DE L'ACCÈS AUX DONNÉES À CARACTÈRE PERSONNEL PAR UN COMITÉ SECTORIEL

Comme la loi BCV le mentionne explicitement[9], l'accès aux données « véhicules » doit être autorisé par le Comité sectoriel pour l'autorité fédérale, qui est un des cinq comités sectoriels institués au sein de la CPVP[10]. Ces comités sectoriels sont des organes indépendants, composés notamment d'experts des secteurs concernés, qui jouent le rôle de « chien de garde » des sources authentiques dont ils contrôlent l'accès[11]. Concrètement, cela signifie qu'il ne suffit plus d'appeler un membre d'une administration qui a accès aux données recherchées en lui demandant de les communiquer par téléphone, par exemple. L'autorisation du comité sectoriel compétent est désormais obligatoire, dans le but de veiller, au cas par cas, à ce que les transferts de données entre administrations soient conformes au régime juridique de la protection de la vie privée. Les décisions des comités sectoriels, publiées en ligne, permettent aussi d'organiser davantage de clarté dans les flux de données, puisque ceux-ci sont ainsi connus et peuvent être répertoriés.

C'est pourquoi, en l'espèce, la Cour de cassation a affirmé que « le fait qu'il relève de la

5 Au sujet de la notion de sources authentiques de données, voy. E. Degrave, *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle,* Bruxelles, Larcier, 2014, nos 13 et s. et réf. citées, en particulier la recommandation de la CPVP n° 09/2012 du 23 mai 2012 relative aux sources authentiques de données dans le secteur public.

6 Art. 6, 1°, de l'arrêté royal du 8 juillet 2013 portant exécution de la loi du 19 mai 2010 portant création de la Banque-Carrefour des véhicules.

7 Art. 5, 7°, de la loi BCV.

8 Voy. l'arrêté royal du 8 juillet 2013, précité, en particulier les articles 6 et 9.

9 Art. 18, § 1er, de la loi BCV.

10 Pour plus de détails sur les comités sectoriels, voy. https://www.privacycommission.be/fr/comites-sectoriels. Le comité sectoriel pour l'autorité fédérale est institué par l'article 36*bis* de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 18 mars 1993.

11 Sur les comités sectoriels, voy. E. Degrave, *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle, op. cit.,* nos 534 et s.

mission de police de rechercher et de constater les infractions de roulage n'implique pas que la police puisse identifier le titulaire d'une plaque d'immatriculation via la DIV sans avoir l'autorisation du comité sectoriel d'accéder aux données à caractère personnel de la Banque-Carrefour des véhicules »[12]. En d'autres termes, même si la police dispose de la compétence légale de traiter les données à caractère personnel des citoyens pour l'exercice de ses missions[13], elle doit être autorisée par le comité sectoriel pour l'autorité fédérale à consulter les données « véhicules », au cas par cas.

Néanmoins, cette affirmation de la Cour est surprenante. Elle semble faire fi d'une exception organisée au bénéfice des services de police, comme le souligne le président du comité sectoriel pour l'autorité fédérale[14]. En effet, un arrêté royal du 4 juin 2003 affirme que « les communications électroniques de données personnelles effectuées par les services de police, dans l'exercice des missions qui leur sont confiées, conformément aux articles 44/1 à 44/11 de la loi du 5 août 1992 sur la fonction de police, sont dispensées de toute autorisation du comité sectoriel pour l'autorité fédérale créé au sein de la Commission de la protection de la vie privée »[15]. Cette exception repose sur l'idée que si l'autorisation d'un comité sectoriel était obligatoire et qu'elle faisait défaut, cela poserait des questions de recevabilité d'éléments de preuve pouvant nuire à l'exercice des missions judiciaires[16]. En outre, un « organe de contrôle de l'information policière » est rattaché à la Commission de la protection de la vie privée qui, selon le président du comité sectoriel pour l'autorité fédérale, constitue un « encadrement plus strict [que celui d'un comité sectoriel] mais respectueux de l'action judiciaire et de police administrative »[17].

Certes, ladite exception a été organisée en 2003, soit antérieurement à la loi BCV de 2010. Néanmoins, d'une part, la loi de 2010 ne fait qu'organiser le réseau sectoriel de la BCV et l'intégrateur de service qu'est la BCV, mais n'apporte pas de modification de fond concernant l'échange des données à caractère personnel qui amènerait à devoir réévaluer éventuellement la raison d'être de l'exception précitée. D'autre part, la loi BCV habilite le Roi à « déterminer les cas dans lesquels une autorisation n'est pas requise » et n'empêche donc pas l'existence de cette exception organisée par arrêté royal.

Quoi qu'il en soit, deux jours après le prononcé de l'arrêt commenté, les services de police ont introduit la demande d'autorisation au comité sectoriel pour l'autorité fédérale, qui s'est prononcé dans l'urgence, le jour-même, en autorisant « la communication des données à caractère personnel de la DIV vers les services de police dans le respect et les limites des dispositions légales et réglementaires qui s'appliquent »[18]. Par conséquent, l'accès par

12 Cass., 13 décembre 2016, n° 7 (traduction libre).

13 Voy. l'article 44/1 de la loi sur la fonction de police.

14 Rapport du Président du Comité sectoriel Stefan Vershuere, en annexe de la délibération AF 53/2016 du 15 décembre 2016 relative à une demande d'autorisation de la Direction de l'information policière et des moyens ICT (DRI) de la Police Fédérale de communication électronique de données de la DIV nécessaires à la police intégrée afin d'exercer ses missions de police judiciaire et administrative, p. 13.

15 Art. 1er de l'arrêté royal du 4 juin 2003 fixant dérogation à l'autorisation visée à l'article 36*bis* de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel au profit de la banque de données nationale générale de la police intégrée structurée à deux niveaux.

16 Rapport au Roi de l'arrêté royal du 4 juin 2003 précité.

17 Rapport du Président du Comité sectoriel Stefan Vershuere, précité, p. 14.

18 Délibération AF 53/2016 du 15 décembre 2016 relative à une demande d'autorisation de la Direction de l'information policière et des moyens ICT (DRI) de la Police Fédérale de communication électronique de données de la DIV nécessaires à la police intégrée afin

les services de police aux données de la DIV est désormais couvert par une autorisation du comité sectoriel pour l'autorité fédérale, bien que demeure la question de savoir si une telle autorisation était légalement nécessaire. Par ailleurs, le législateur a souhaité récemment clarifier tout à fait les choses en modifiant l'article 36*bis* de la loi du 8 décembre 1992. Celui-ci est complété d'un alinéa affirmant que « dans l'exercice de leurs missions de police administrative et de police judiciaire, les services de police tels que définis à l'article 2, 2°, de la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux sont dispensés de toute autorisation préalable du comité sectoriel ». Il est à noter que cette loi rétroagit au 2 juin 2003, soit à la date de l'entrée en vigueur de la loi qui a notamment créé le comité sectoriel pour l'autorité fédérale[19].

Au-delà de ce cas d'espèce, signalons que la demande d'autorisation adressée au comité sectoriel prend la forme d'un formulaire à remplir, disponible sur le site de la Commission de la protection de la vie privée[20]. À cette occasion, le demandeur doit préciser les éléments essentiels du traitement de données envisagé, tels que les finalités déterminées et légitimes poursuivies, les données demandées, la fréquence de l'accès aux données demandé, les catégories de personnes qui auront accès aux données, etc.

Au terme de cet examen, le comité sectoriel rend une décision qui a force obligatoire. Cela signifie qu'en cas de refus d'autorisation, le demandeur ne pourra pas accéder aux données réclamées. Peut-il attaquer pareil refus d'autorisation en justice ? À notre connaissance, aucun recours de ce type n'a encore été introduit. Or, selon nous, les décisions des comités sectoriels doivent pouvoir être attaquées devant le Conseil d'État, section du contentieux administratif, dès lors que ces décisions s'apparentent aux décisions des autorités administratives au sens de l'article 14 des lois coordonnées sur le Conseil d'État[21]. La directive européenne relative à la protection des données[22] et le règlement général de protection des données[23] qui la remplacera dès le 25 mai 2018 exigent d'ailleurs que les décisions des autorités de contrôle puissent faire l'objet d'un recours en justice. On peut donc raisonnablement penser qu'un recours intenté contre une décision de comité sectoriel soit déclaré recevable par le Conseil d'État.

III. LES CONSÉQUENCES DU NON-RESPECT DE LA PROCÉDURE D'AUTORISATION

Suite à cet arrêt de la Cour de cassation, la question s'est posée de savoir si les conducteurs à qui un procès-verbal avait été envoyé après une consultation illégale des données

d'exercer ses missions de police judiciaire et administrative, p. 10.

19 Loi du 26 février 2003 modifiant la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale en vue d'aménager le statut et d'étendre les compétences de la Commission de la protection de la vie privée, *M.B.*, 26 juin 2003.

20 Ce formulaire est disponible à l'adresse https://www.privacycommission.be/fr/procedure-autorisation-af.

21 Au sujet de la recevabilité des recours intentés contre les décisions des comités sectoriels de la CPVP, voy. E. Degrave, *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle, op. cit.*, n^os^ 575 et s.

22 Art. 28 de la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données.

23 Art. 78 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE.

de la DIV pouvaient se réjouir de ne pas devoir payer ledit PV[24].

Il revient désormais aux juges de fond de se prononcer au cas par cas[25]. Néanmoins, les contrevenants ne doivent pas se réjouir trop vite. L'excès de vitesse originaire a bien eu lieu et a été constaté régulièrement par caméra. Seul l'envoi du PV est irrégulier puisqu'il est fondé sur une consultation illégale de l'identité et de l'adresse du conducteur concerné. C'est donc la manière dont la preuve de l'identité du conducteur a été obtenue qui est illégale, mais non la constatation de l'infraction qui a été effectivement commise.

Or, l'article 32 du Titre préliminaire du Code d'instruction préliminaire, qui ancre légalement la jurisprudence dite « Antigone », est applicable aux preuves illégalement obtenues. Selon cette disposition, « la nullité d'un élément de preuve obtenu irrégulièrement n'est décidée que si :

– le respect des conditions formelles concernées est prescrit à peine de nullité, ou ;
– l'irrégularité commise a entaché la fiabilité de la preuve, ou ;
– l'usage de la preuve est contraire au droit à un procès équitable ».

Il reste à voir comment les juges du fond saisis de ces litiges interpréteront cet article 32. Certains se sont déjà prononcés, comme le tribunal de police de Leuven[26]. Celui-ci était saisi d'un cas similaire, un conducteur ayant commis un excès de vitesse, dont les données à caractère personnel avaient été consultées illégalement par la police. Ce tribunal s'est prononcé deux jours après l'arrêt de la Cour de cassation. Il a fait application dudit article 32, et décidé qu'aucune des hypothèses de nullité de la preuve n'était rencontrée dans ce cas. Il a jugé que l'obtention d'une autorisation du comité sectoriel pour l'autorité fédérale n'est pas une condition prescrite à peine de nullité. Et que l'accès illégal aux données de la DIV n'entache pas la fiabilité de la preuve obtenue. Enfin, le tribunal a considéré qu'il n'y avait pas d'atteinte au procès équitable compte tenu du fait que les services de police n'avaient pas commis l'illégalité de manière délibérée et que, les excès de vitesse étant une des causes principales d'accidents de la route, la sécurité routière importe plus qu'une éventuelle atteinte à la vie privée[27].

IV. UNE PROCÉDURE D'AUTORISATION SYMBOLIQUE ?

Ainsi donc, le fait, pour les services de police verbalisant, d'avoir consulté les données à caractère personnel des contrevenants sans autorité du comité sectoriel compétent et d'avoir de ce fait agi illégalement, n'empêchera vraisemblablement pas, au final, la perception de l'amende due pour l'excès de vitesse commis.

Mais alors, de manière générale, au-delà de cette hypothèse, doit-on en conclure que le non-respect de la procédure d'autorisation du comité sectoriel compétent n'entraîne pas de conséquence concrète ? Cette procédure ne serait-elle que symbolique ?

Ce serait tirer des conclusions fort hâtives.

En effet, si la preuve obtenue illégalement peut tout de même être utilisée en justice par application de l'article 32 précité, cela ne signifie pas que l'illégalité commise dans la consultation

[24] Voy. not. http://www.lalibre.be/actu/belgique/denombreuses-amendes-routieres-peut-etre-illegales-5852f137cd701e2eb2881ba8.

[25] Dans le même sens, T. Souverijs, « Hof van Cassatie verklaart opvragen persoonsgegevens onwettig », *Juristenkrant*, 21 décembre 2016, p. 2.

[26] À ce sujet, voy. S. Royer, « Identificatie houder kentekenplaat », *NjW*, 15 février 2017, p. 116.

[27] *De Standaard*, « Politierechtbank: 'Verkeersveiligheid primeert op schending privacy' », 15 décembre 2016.

des données à caractère personnel est sans conséquence.

En consultant les données des citoyens sans avoir obtenu l'autorisation du comité sectoriel compétent, l'administration commet une illégalité. Une telle illégalité est une faute, au sens de l'article 1382 du Code civil, selon une jurisprudence constante de la Cour de cassation largement commentée en doctrine[28]. Cette faute pourrait provoquer un dommage qui ne se serait pas produit tel qu'il s'est produit si la consultation illégale de données n'avait pas eu lieu. On pense, par exemple, au cas récent d'un policier qui consultait illégalement des bases de données pour obtenir la photo et le numéro de GSM de femmes qu'il avait repérées lors de contrôles routiers. Il les harcelait ensuite par SMS[29]. Sans la consultation illégale de données, le policier n'aurait probablement pas pu connaître le numéro de GSM et commettre ces harcèlements dommageables.

Par ailleurs, l'article 15*bis* de la loi du 8 décembre 1992 et l'article 82 du règlement général sur la protection des données (« RGPD ») bientôt en application, aboutissent à un résultat similaire en affirmant que « toute personne ayant subi un dommage matériel ou moral du fait d'une violation du présent règlement a le droit d'obtenir du responsable du traitement ou du sous-traitant réparation du préjudice subi »[30].

Enfin, d'ici quelques mois, lorsque le RGPD sera d'application, la Commission de la protection de la vie privée disposera du pouvoir d'adopter des mesures correctrices qui pourraient s'avérer utiles face à de telles illégalités : avertir le responsable de traitement, le rappeler à l'ordre, lui ordonner de se mettre en conformité avec le RGPD, imposer une limitation de traitement, qui peut être définitive, etc.[31]. Et surtout, la Commission de la protection de la vie privée disposera du pouvoir d'imposer une amende, notamment aux administrations, d'un montant particulièrement dissuasif pouvant aller jusqu'à 20.000.000 euros[32].

CONCLUSION

Contrairement à ce qu'ont espéré certains conducteurs, l'arrêt de la Cour de cassation ne fera vraisemblablement pas obstacle au paiement des amendes réclamées, quand bien même celles-ci ont pu être envoyées à

28 À ce sujet, voy. Cass., 19 décembre 1980, *Pas.*, 1981, I, p. 453 ; Cass., 13 mai 1982, *J.T.*, 1982, p. 772 et R.-O. Dalcq, obs. sous Cass., 13 mai 1982, *R.C.J.B.*, 1984, pp. 19 à 31 ; voy. égal. J.-L. Fagnart, « La responsabilité de l'administration du chef d'excès de pouvoir », obs. sous Bruxelles, 14 septembre 1979, *A.P.T.*, 1980, pp. 56 à 62 ; du même auteur, « De la légalité à l'égalité », in *La responsabilité des pouvoirs publics,* Bruxelles, Bruylant, 1991, p. 23 ; H. Vandenberghe, « Overheidsaansprakelijkheid. Aansprakelijkheid van de uitvoerende macht », in *Overheidsaansprakelijkheid* (dir. H. Vandenberghe, A. Van Oevelen, H. Vuye, L. Wynant et H. Vandenberghe), Bruges, die Keure, 2005, pp. 7 et s. ; B. Dubuisson, « Faute, illégalité et erreur d'interprétation en droit de la responsabilité civile », note sous Cass. (1re ch.), 26 juin 1998, *R.C.J.B.*, 2001, pp. 28 à 72 ; D. De Roy, « La responsabilité quasi délictuelle de l'administration : unité ou dualité des notions d'illégalité et de faute ? », in *La protection juridictionnelle du citoyen face à l'administration* (dir. H. Dumont, P. Jadoul et S. van Drooghenbroeck), Bruxelles, la Charte, 2007, pp. 69 à 108 ; C. Doyen-Biver, A. L. Durviaux, D. Fisse, J. Sohier, *La responsabilité des pouvoirs publics,* Kluwer, Waterloo, 2010.

29 https://www.rtbf.be/info/regions/detail_un-an-avec-sursis-pour-un-policier-qui-profitait-de-ses-fonctions-pour-harceler-des-dames?id=9546926.

30 Art. 82 RGPD. L'article 15*bis* de la loi du 8 décembre 1992 est formulé comme suit « lorsque la personne concernée subit un dommage causé par un acte contraire aux dispositions déterminées par ou en vertu de la présente loi, les alinéas 2 et 3 ci-après s'appliquent, sans préjudice d'actions fondées sur d'autres dispositions légales. Le responsable du traitement est responsable du dommage causé par un acte contraire aux dispositions déterminées par ou en vertu de la présente loi. Il est exonéré de cette responsabilité s'il prouve que le fait qui a provoqué le dommage ne lui est pas imputable ».

31 Art. 58 RGPD.

32 Art. 83 RGPD.

leur destinataire grâce à un accès illégal aux données de la DIV.

Néanmoins, cet arrêt a le mérite de rappeler que les données à caractère personnel que détient l'État sont soumises à une protection stricte, même si certaines données comme l'adresse ou le numéro de plaque d'immatriculation peuvent paraître anodines. Ainsi donc, le temps est révolu, où les agents de l'administration se téléphonaient entre eux pour obtenir la communication de données dont ils avaient besoin. Désormais, l'accès aux données des citoyens est soumis à l'obtention d'une autorisation du comité sectoriel compétent, qui vise à assurer davantage de clarté et de légalité dans le traitement desdites données.

En outre, bien que, comme le montre l'affaire commentée, une preuve illégale n'est pas nécessairement annulée, le non-respect de la procédure d'autorisation peut conduire à d'autres types de sanctions, qui seront prochainement renforcées dès l'entrée en application du RGPD, le 25 mai 2018. Gageons du fait que les administrations n'auront pas à les subir.

Elise Degrave