# Employés pucés et vie privée

Degrave, Élise

*Published in:*
Journal des Tribunaux

*Publication date:*
2017

*Document Version*
le PDF de l'éditeur

Bureau de dépôt : Louvain 1
Hebdomadaire, sauf juillet et août
ISSN 0021-812X
P301031

larcier

Journal des tribunaux

http://jt.larcier.be
29 avril 2017 - 136e année
16 - No 6686
Georges-Albert Dal, rédacteur en chef

## Sommaire

### Doctrine



### Jurisprudence



### Chronique





Doctrine

# Employés pucés et vie privée

Récemment, des employés d'une société de marketing digital malinoise, la société Newfusion, se sont vus implanter une puce dite « RFID » sous la peau. Cette puce leur permet d'accéder aux locaux de la société et d'ouvrir leur ordinateur. Une telle méthode respecte-t-elle les droits et libertés fondamentaux des employés concernés ? C'est à cette question qu'est consacrée la présente étude[1].

## 1 Qu'est-ce qu'une puce RFID ?

Une puce RFID (pour *Radio Frenquency IDentification*) est un dispositif micro-électronique, constitué d'une puce informatique munie d'une antenne, qui peut être activée à distance par un lecteur et communiquer avec celui-ci grâce à un signal électromagnétique. Sa particularité est qu'elle n'a pas besoin d'être vue pour être lue, à la différence d'un code-barre, ni d'entrer en contact physique avec un lecteur, à la différence d'une carte bancaire. Selon les types de puces, il est possible de la lire à quelques centimètres voire quelques dizaines de mètres. La plupart des puces n'ont pas besoin de pile. Les signaux électromagnétiques qu'envoient le lecteur à la puce lui donnent l'énergie suffisante pour communiquer avec lui. Quant à leur contenu, beaucoup de puces sont simples et intègrent uniquement un numéro d'identification pouvant être lu par le lecteur. Certaines peuvent néanmoins contenir des données supplémentaires, comme les données d'identification d'une personne ou ses données santé[2]. La puce implantée dans les employés de la société Newfusion contient un numéro d'identification. Dans la base de données de l'entreprise figure le lien entre ce numéro d'identification et l'identité de l'employé porteur de la puce. En outre, cette puce intègre une mémoire de 800 bytes contenant la carte de visite de l'employé[3].

Nous utilisons les puces RFID au quotidien. Elles sont présentes dans les clés sans contact des voitures et les badges d'accès aux immeubles. Intégrées dans des étiquettes collées sur des produits, elles servent d'antivol faisant sonner le portique de sécurité, facilitent le contrôle des flux de marchandisages et la constitution des inventaires, permettent de scanner, sans les manipuler, chaque produit qui passe en caisse. Par ailleurs, des bracelets de surveillance contenant une puce RFID sont utilisés dans des maisons de repos comme « dispositif anti-errance »[4], ou placés sur des nourrissons en maternité pour lutter contre le rapt d'enfant ou l'échange de bébés[5].

Depuis quelques années, émergent des cas de puces RFID implantées sous la peau des personnes. La société belge qui l'a fait récemment n'est pas un précurseur en la matière. En 2004, en Espagne, une boîte de nuit de Barcelone proposait à ses clients de leur injecter dans le bras une puce pour 125 EUR, qui leur permettait d'accéder au carré VIP et de payer leurs consommations en passant

(1) Signalons que ce sujet en a fait l'objet, le 3 février 2017, d'une question orale de Benoit Hellings, député, à Philippe De Backer, sécrétaire d'État à la Lutte contre la fraude sociale, à la Protection de la vie privée et à la Mer du Nord. Ce dernier n'y a pas encore répondu. La question est accessible à l'adresse suivante : http://benoithellings.be/20170203%20QO%20De%20Backer%20Puce%20Incorpor%C3%A9e.pdf. Par ailleurs, à la suite d'une interpellation du député Georges Gilkinet, le ministre Kris Peeters a annoncé avoir saisi le Conseil national du travail le 22 mars dernier pour avoir son avis sur cette question. Voy. http://www.georges-gilkinet.be/?travailleurs-puces-le-conseil.

(2) Pour plus d'informations sur la notion de puce RFID voy. notamment la recommandation de la Commission européenne du 12 mai 2009 sur la mise en œuvre des principes de respect de la vie privée et de protection des données dans les applications reposant sur l'identification par radiofréquence, 16 mai 2009, L. 122/47, no 3 ; CNIL, « Des puces aux usages multiples et aux impacts variés en termes de vie privée », 26 septembre 2013 disponible à l'adresse suivante : https://www.cnil.fr/fr/rfid-des-puces-aux-usages-multiples-et-aux-impacts-varies-en-termes-de-vie-privee-0 ; proposition de résolution relative à la sécurisation des supports électroniques de données, *Doc. parl.*, Chambre, sess. ord. 2014-2015, no 54-0065/001, p. 3 ; R. LEFEBURE, « La technologie du tag RFID et leur utilisation », http://www.blog-crm.fr/exposes-etudiants/technologie-rfid/ ; F. GRÉGOIRE, « Puces FRID, le cœur de l'intelligence du tag RFID », http://www.companeo.com/portiques-de-securite/guide/puces-rfid-tag-badge-etiquette#0.

(3) Information qui nous a été communiquée par la société Newfusion le 10 mars 2017.

(4) N. GUBERT, « Surveillance par bracelet électronique dans une maison de retraite de Lille », http://www.lepoint.fr/actualites-societe/2009-05-22/surveillance-par-bracelet-electronique-dans-une-maison-de/920/0/345772.

(5) TIC Santé, « Un dispositif de traçabilité pour les nourrissons », http://www.ticsante.com/Un-dispositif-de-tracabilite-du-nourrisson-avec-la-RFID-NS_242.html.

leur bras près d'un lecteur[6]. En Suède, en 2015, plusieurs employés de la société Epicenter ont accepté qu'on leur place une puce dans la main pour accéder aux locaux et utiliser la photocopieuse[7]. Depuis 2016, un club de football canadien propose à ses abonnés de « porter le club en eux » grâce au « ticket passion », une puce implantée dans le bras qui permet d'accéder au stade sans billet ni carte d'identité[8].

## 2 Un enjeu pour la protection de la vie privée des citoyens

L'usage d'une puce RFID touche à la question de la protection de la vie privée dès le moment où il est possible, par des moyens raisonnables, d'identifier une personne au départ de cette puce. Cela peut se faire de plusieurs manières[9].

Soit la puce contient en elle-même des données à caractère personnel et il suffit de la lire pour identifier la personne concernée. C'est le cas, par exemple, de la carte de transport MOBIB de la Stib, qui contient les nom, prénom, date de naissance et code postal du domicile du propriétaire de la carte. Soit la puce ne contient qu'un numéro d'identification qui n'est pas, en lui-même, une donnée à caractère personnel mais qui le devient dès lors qu'il est possible de rattacher ce numéro à un individu. C'est ce qu'il se passe lorsqu'un magasin fait le lien entre le numéro d'identification d'un produit et les données du client qui l'a acheté et est enregistré dans la base de données du magasin. Ce type d'opération est réalisé pour rappeler des produits défectueux, notamment.

Dans chacune de ces hypothèses, la lecture de la puce RFID constitue un traitement de données à caractère personnel. Il s'impose alors de respecter les règles de protection des données à caractère personnel organisées par la loi du 8 décembre 1992 sur la protection de la vie privée à l'égard des traitements de données à caractère personnel (dite « loi vie privée »)[10].

Néanmoins, le cas de la puce RFID implantée sous la peau d'un employé d'une entreprise présente des particularités qui justifient qu'une attention particulière soit portée à certaines exigences de la loi vie privée. L'analyse qui suit est consacrée à cette hypothèse.

## 3 Le respect des règles de protection des données à caractère personnel

Ainsi donc, injecter une puce RFID sous la peau d'un employé suppose de respecter les règles de protection des données à caractère personnel. Parmi ces règles, deux exigences retiennent particulièrement l'attention en l'espèce. Il s'agit, d'une part, de la proportionnalité du traitement de données au regard de l'objectif poursuivi et, d'autre part, du consentement de l'employé.

### A. La proportionnalité du traitement au regard de l'objectif poursuivi

Que ce soit au sein de la société belge qui a implanté huit employés, ou de la société suédoise qui a utilisé le même procédé auparavant, les objectifs annoncés par ces entreprises touchent à la facilitation des tâches quotidiennes des employés quant à l'accès au bâtiment de l'entreprise, l'usage de la photocopieuse, l'ouverture de l'ordinateur des employés concernés.

Or, en vertu de l'article 8 de la Convention européenne des droits de l'homme qui fonde le régime juridique de la protection de la vie privée et des données à caractère personnel, toute ingérence dans la vie privée des citoyens doit être « nécessaire dans une société démocratique ». La version modernisée de la Convention 108[11] pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel précise cette exigence en affirmant que « le traitement de données doit être proportionné à la finalité légitime poursuivie et refléter à chaque étape du traitement un juste équilibre entre tous les intérêts en présence, qu'ils soient publics ou privés, ainsi que les droits et les libertés en jeu »[12].

Cela suppose d'examiner si le moyen utilisé, en l'occurrence l'implantation d'une puce dans le corps, est proportionné aux objectifs poursuivis. En d'autres termes, comme le rappelle la Commission de la protection de la vie privée, il y a lieu de vérifier « que l'objectif pour lequel les données à caractère personnel sont traitées ne peut pas être réalisé d'une autre manière moins désavantageuse pour la personne concernée »[13], ce qui se fait notamment en comparant la puce sous-cutanée à d'autres méthodes déjà existantes.

Force est de constater qu'implanter une puce RFID sous la peau d'un employé menace sa *vie privée* sur le lieu de travail. Si des lecteurs de puces se situent à plusieurs endroits de l'entreprise, ils enregistrent le passage de la personne à tel endroit à tel moment, données desquelles il est ensuite possible de déduire l'heure d'arrivée au travail, la durée des pauses de l'employé, le nombre de passages aux toilettes, la durée du repas pris dans le restaurant de l'entreprise, le nombre et la durée des sorties du bâtiment, etc. Étant donné que la puce ne peut pas être détachée à la fin de la journée de travail, l'individu concerné peut également être tracé en dehors de l'entreprise. Cela dépendra du type de puce. Les puces simples, contenant uniquement un numéro d'identification, transmettent leur identifiant à n'importe quel lecteur. D'autres puces sont plus sécurisées. Leur lecture nécessité au préalable l'authentification du lecteur. Dans ce cas, les données ne seront envoyées que si le lecteur est connu de la puce. Ce type de puce est néanmoins plus complexe et surtout plus cher[14].

Par ailleurs, la *sécurité* des données n'est pas nécessairement garantie. Cela dépend de la technologie utilisée, qui peut être plus au moins sécurisée. En effet, les données stockées sur la puce ne sont pas nécessairement cryptées. Certaines sont juste codées et pourront être décodées, ou même simplement enregistrées en clair, lisibles facilement[15]. Des expériences ont d'ailleurs montré que certaines puces RFID sont facilement lisibles par des tiers[16]. Aux États-Unis, par exemple, un chercheur informaticien a craqué la sécurité d'une puce RFID sous-cutanée, en a lu les données et les a clonées en moins de deux heures, parvenant alors à accéder à tous les endroits et services accessibles avec la puce, et disposant également d'une copie des données médicales qui figuraient sur cette puce[17]. Par ailleurs, la vie privée de la personne concernée risque d'être d'autant plus atteinte en cas de détournement de la finalité d'utilisation de la puce, facilité par des failles de sécurité. On peut ainsi craindre que des individus peu scrupuleux[18] soient tentés d'utiliser les informations de la puce pour traquer voire persécuter les militants des droits de l'homme, les opposants politiques, les migrants, notamment.

Au-delà de la protection de la vie privée et des données à caractère personnel, l'implantation d'une puce RFID dans le corps menace la

(6) http://www.courrierinternational.com/article/2004/06/03/une-puce-electronique-sous-la-peau-pour-entrer-en-discotheque.
(7) G. Sylvain, « En Suède, une entreprise implante des puces à ses salariés pour réduire la queue à la photocopieuse », https://aruco.com/2015/02/epicenter-puce-peau/.
(8) http://www.lapresse.ca/actualites/insolite/201604/26/01-4975217-une-puce-sous-la-peau-pour-entrer-au-stade.php.
(9) CPVP, avis n° 27/2009 du 28 octobre 2009, d'initiative relatif à la RFID, n^os 10-12.
(10) Pour l'heure, ces exigences sont organisées par la loi vie privée qui, dès la fin du mois de mai 2018, sera remplacée par le règlement européen général sur la protection des données à caractère personnel. Néanmoins, en l'occurrence, les textes affirment sensiblement la même chose.
(11) Cette version est actuellement dans sa dernière phase d'adoption.
(12) Article 5 de la version modernisée de la Convention n° 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. La dernière version de ce texte, datée de septembre 2016, est accessible ici https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806b6f7b.
(13) CPVP, avis n° 27/2009 précité, n^os 25-26.
(14) Entretien avec le professeur Jean-Noël Colin, professeur à la Faculté d'informatique de l'Université de Namur.
(15) Idem.
(16) Council on ethical and judicial affairs, *Report about Radio Frequency ID Devices in Human*, 5-A-07, pp. 2-3 accessible à l'adresse https://www.privacycoalition.org/ama-report.pdf.
(17) A. Newitz, « The RFID Hacking Underground », 5 janvier 2006, https://www.wired.com/2006/05/rfid-2/.
(18) Dont certains peuvent se retrouver à la tête des plus grandes puissances mondiales...

*santé* des individus. Pour le moment, peu d'études ont été menées à ce sujet. Néanmoins, un rapport de la « Food and Drug Administration » aux États-Unis énonce les risques potentiels de ce dispositif : « réaction dermatologique ; migration du transpondeur implanté ; défaillance de l'applicateur ; défaillance du scanner électronique ; perturbations électromagnétiques ; risques électriques ; incompatibilité avec l'imagerie par résonance magnétique ; blessure par l'aiguille »[19].

Enfin, on ne doit pas ignorer que la puce sous-cutanée pose question au regard de l'*inviolabilité du corps humain* et, plus largement, de la *dignité humaine*, deux principes juridiquement contraignants consacrés, entre autres, par la Charte des droits fondamentaux de l'Union européenne[20]. Au départ notamment de ces deux valeurs fondamentales, le Groupe européen d'éthique des sciences et des nouvelles technologies (« GEE ») institué auprès de la Commission européenne a rendu un avis sur « les aspects éthiques des implants TIC dans le corps humain »[21], qui vise notamment les puces RFID sous-cutanées. Le GEE y affirme que les « règles juridiques servent généralement de garde-fou aux dérives technologiques et à rappeler que tout ce qui est techniquement possible n'est pas nécessairement admissible sur le plan éthique, socialement acceptable, ni légalement approuvé »[22]. D'un point de vue éthique plus particulièrement, le GEE énonce que « chaque intervention sur le corps, chaque opération de traitement de données à caractère personnel doit être considérée comme touchant le corps dans son ensemble, comme touchant un individu qui doit être respecté dans son intégrité à la fois physique et mentale. C'est là un nouveau concept global de l'individu, et sa traduction dans la réalité donne le droit de revendiquer le respect total d'un corps qui, aujourd'hui, est à la fois physique et électronique »[23]. Et de soutenir ensuite que « les applications non médicales des implants TIC sont une menace potentielle pour la dignité humaine et la société démocratique »[24]. Le GEE appelle à une vigilance particulière concernant notamment le respect de l'exigence de proportionnalité et du consentement libre et éclairé[25].

Ainsi donc, même si la puce RFID sous-cutanée permet de faciliter certaines tâches au travail, elle n'en demeure pas moins très problématique au regard du critère de proportionnalité. De toute évidence, cette puce génère des risques non négligeables d'atteinte aux droits et libertés des individus concernés. Or il existe des méthodes moins invasives qui permettent d'atteindre les mêmes objectifs. On pense à l'usage d'un badge, qui pourrait même prendre la forme d'un bracelet de festival de musique, léger et qu'on est libre de garder, ou pas, au poignet. On pense également à la mémorisation d'un code d'accès. Quand bien même le travailleur oublierait ce badge ou ce code d'accès, les conséquences de tels oublis seraient bien plus limitées dans le temps et dans l'espace, et donc au final moins néfastes, que celles attachées à l'implantation d'une puce dans le corps.

### B. Le consentement de l'employé

Obtenir le consentement de l'employé qui va être implanté est une autre obligation issue du régime juridique de la protection de la vie privée et des données à caractère personnel. L'article 7 de la directive 95/46[26], transposé en droit belge par l'article 5 de la loi vie privée, énonce les cas dans lesquels un traitement de données peut être effectué. Parmi ceux-ci, le fait que « la personne concernée a indubitablement donné son consentement » est applicable en l'espèce. L'article 1er, § 8, de la loi vie privée définit le consentement de la personne concernée comme « toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée ou son représentant légal accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement »[27]. En d'autres termes, l'employé doit avoir donné son consentement avant d'être implanté, et ce consentement doit être libre, spécifique et informé.

Or le consentement donné par un employé à son patron est-il vraiment *libre* ? Selon la Commission de la protection de la vie privée, « un consentement libre implique entre autres qu'un système alternatif soit proposé à la personne concernée lequel doit être équivalent et ne peut impliquer aucune sanction pour la personne concernée »[28]. Ainsi donc, l'employé doit avoir le choix entre se faire implanter une puce ou disposer d'un autre moyen d'accéder aux locaux de son entreprise, d'ouvrir son ordinateur et d'utiliser la photocopieuse. Dans les faits néanmoins, quand bien même l'employé aurait le choix, il est difficile de savoir si aucune pression n'est effectuée sur lui pour l'inciter à choisir la puce RFID. Cette pression pourrait même émaner simplement du fait que la plupart de ses collègues ont opté pour la puce RFID et qu'il n'ose pas agir différemment ou que, par conscience professionnelle, il ne souhaite pas décevoir son patron. Par ailleurs, le risque se présente également dans le processus d'engagement. Accepter la puce RFID pourrait être érigé comme une condition d'accès à l'emploi, forçant alors le consentement d'un candidat au poste.

Pour que le consentement soit libre, il doit aussi pouvoir être retiré ce qui, en l'espèce, suppose une opération chirurgicale. Celle-ci devra donc être financée par l'employeur, comme corollaire de l'implantation de la puce. Comment faire alors en cas de faillite de la société, par exemple ?

Par ailleurs, comment rendre le consentement *spécifique et informé* ? Pour informer l'employé de ce à quoi il consent, l'employeur doit respecter l'obligation d'information de la personne concernée par le traitement de données à caractère personnel mis en place, conformément à l'article 9 de la loi vie privée. C'est d'une « importance extrême étant donné la possibilité de traiter des données "invisibles" en utilisant les [puces RFID] »[29]. Dès lors, il faut fournir à l'employé une information précise sur les finalités d'utilisation de la puce, les données qui y seront enregistrées, les personnes qui auront accès à ces données. Il faut également informer l'employé de son droit d'accès et de rectification à toutes les données enregistrées sur la puce et à l'aide de la puce. En outre, pour que le consentement de l'employé soit spécifique, ce dernier doit être conscient des risques éventuels de la puce pour sa santé, et savoir qu'il existe des risques de failles de sécurité engendrant des détournements de ses données[30].

## Conclusion

Force est de constater qu'implanter une puce RFID dans le corps d'un employé pose problème à plusieurs égards. D'une part, il s'agit d'une méthode particulièrement invasive, qui présente des risques d'atteinte à la vie privée, à la santé, à la dignité humaine. L'examen de proportionnalité de cette méthode a révélé qu'il n'est pas nécessaire d'y recourir pour faciliter des tâches aussi simples qu'ouvrir une porte, un ordinateur ou utiliser une photocopieuse. L'usage d'un badge ou la mémorisation d'un code d'accès suffit.

Par ailleurs, ce dispositif suppose l'obtention du consentement libre, spécifique et informé de l'employé. Or, parmi les difficultés que soulèvent cet impératif juridique, il est difficile voire impossible de garan-

**(19)** Food and Drug Administration, Department of Health and Human Services, « Evaluation of Automatic Class III Designation Verichip (tm) Health Infomation Microtransponder System », 12 octobre 2004, p. 3.
**(20)** Voy. en particulier, les articles 1 et 3. Depuis l'entrée en vigueur du Traité de Lisbonne le 1er décembre 2009, la Charte des droits fondamentaux de l'Union européenne a une valeur juridiquement contraignante, comme l'affirme l'article 6 du Traité de l'Union européenne.
**(21)** Groupe européen d'éthique des sciences et des nouvelles technologies auprès de la Commission européenne, avis no 20 « Aspects éthiques des implants TIC dans le corps humain », 16 mars 2005. Bien que cet avis date de 2005, il reste parfaitement d'actualité et est encore régulièrement mentionné dans la littérature à ce sujet.
**(22)** *Ibidem*, p. 32.
**(23)** *Ibidem*, p. 33.
**(24)** *Ibidem*, p. 36.
**(25)** À ce sujet, voy. *infra*.
**(26)** 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 de ces données, *J.O.* L 281 du 23 novembre 1995.
**(27)** Le règlement général de protection des données est encore plus explicite, en affirmant que le consentement est « toute manifestation de volonté libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement » (article 4. 11).
**(28)** CPVP, avis no 27/2009 précité, no 24 ; recommandation de la Commission européenne du 12 mai 2009 sur la mise en œuvre des principes de respect de la vie privée et de protection des données dans les applications reposant sur l'identification par radiofréquence, *op. cit.*, considérant no 23 et article 7.
**(29)** CPVP, avis no 27/2009 précité, no 27.
**(30)** Groupe européen d'éthique des sciences et des nouvelles technologies auprès de la Commission européenne, avis no 20 précité, p. 36 ; Report of the Council on ethical and judicial affaires (USA), *Radio frequency ID Devices in Humans*, 5-A-07, p. 3.

tir que le consentement que donne un employé à son patron soit tout à fait libre vu le déséquilibre existant entre les parties au contrat. À cet égard, le règlement européen général sur la protection des données, qui entrera en vigueur le 25 mai 2018, dispose, en son considérant 43, que « pour garantir que le consentement est donné librement, il convient que celui-ci ne constitue pas un fondement juridique valable pour le traitement de données à caractère personnel dans un cas particulier lorsqu'il existe un déséquilibre manifeste entre la personne concernée et le responsable du traitement ». Ne faut-il pas reconnaître, en l'espèce, l'existence d'un déséquilibre manifeste qui vicie le consentement donné ?

Il appert de l'ensemble de ces éléments qu'implanter un employé dans le cadre d'une relation de travail soulève d'importants problèmes, non seulement par rapport au droit fondamental à la protection de la vie privée et du régime juridique de la protection des données, mais également au regard d'autres enjeux impérieux, tels que la protection de la santé et de la dignité humaine. Gageons que le législateur se montrera réactif à l'expansion de ce dispositif et saura répondre adéquatement aux questions cardinales qu'il soulève en fixant des balises claires pour la protection des citoyens.

Elise DEGRAVE[31]
*Chargée de cours à la Faculté de droit de l'Université de Namur*
*Chercheuse au CRIDS*

**(31)** L'auteure remercie Karen Rosier, avocate et chercheuse au CRIDS (UNamur), Pierre Joassart, avocat et chercheur au CRECO (U.C.L.) ainsi que Yves Poullet et Cécile de Terwangne, professeurs à la Faculté de droit (UNamur) et Jean-Noël Colin, professeur à la Faculté d'informatique (UNamur) pour les avis et idées échangés. Néanmoins, les opinions avancées dans cette étude n'engagent qu'elle-même.



# Indemnité et remboursement anticipé d'un prêt à intérêt

## La Cour de cassation confirme l'application de l'article 1907*bis* du Code civil

Les *funding loss* engendrent un contentieux non négligeable devant les cours et tribunaux, et emportent leur lot de controverses. Parmi celles-ci, une question a longtemps divisé les auteurs de doctrine comme les juridictions du pays : la limitation à 6 mois d'intérêts de l'article 1907bis du Code civil s'applique-t-elle à un contrat de prêt qui n'autorise pas le remboursement anticipé ? Répondant à cette question par un arrêt du 24 novembre 2016 (publié ci-après, p. 298), la Cour de cassation a pleinement rempli sa mission doctrinale en éclairant les juges quant à l'interprétation à donner à cette disposition.

Les indemnités de remploi réclamées lors du remboursement d'un crédit d'investissement, d'une avance à terme ou d'autres formes de crédit professionnel à durée déterminée se révèlent souvent dissuasives. Leur ampleur suscite ainsi un important contentieux judiciaire, auquel la loi Laruelle n'a pas mis totalement fin[1]. Au cœur du débat figure la question de l'application de l'article 1907*bis* du Code civil[2], qui limite à 6 mois d'intérêts l'indemnité pouvant être réclamée lors du remboursement anticipé d'un prêt.

L'article 1907*bis* ne s'applique qu'aux prêts à intérêt[3], à l'exclusion des ouvertures de crédit[4]. Pour pouvoir déterminer si cette disposition trouve ou non à s'appliquer, le juge est ainsi fréquemment appelé à qualifier le crédit litigieux, ou à le requalifier si son libellé ne reflète pas l'intention des parties ou ne correspond pas aux caractéristiques du contrat[5]. Les critères qui permettent de distinguer les prêts des ouvertures de crédit ayant encore récemment fait l'objet de contributions doctrinales de qualité, nous invitons le lecteur à s'y reporter[6].

**(1)** La loi du 21 décembre 2013 relative à diverses dispositions concernant le financement des petites et moyennes entreprises, *M.B.*, 31 décembre 2013, ne s'applique en effet qu'aux crédits conclus après le 10 janvier 2014, exclut certaines entreprises de son champ d'application et n'encadre par ailleurs véritablement les indemnités qu'à l'égard des crédits inférieurs à 1 million d'euros.
**(2)** Appartenant au régime de droit commun du prêt, cette disposition impérative ne concerne pas les crédits visés par des dispositions légales plus spécifiques (*lex specialis*), tel le crédit hypothécaire et le crédit à la consommation.
**(3)** À noter que le caractère réel du contrat de prêt est remis en cause (B. DU LAING, *(Geld)lening en krediet(opening)*, Bruges, die Keure, 2005, spécialement pp. 33-70 – dont la thèse est résumée dans le *R.W.*, 2004-2005, pp. 961-971). Une reconnaissance du caractère consensuel du prêt d'argent (en France, voy. Cass. civ. fr., 28 mars 2000, *J.C.P.*, 2000, II, 10296, p. 753) emporterait une importante raréfaction des hypothèses dans lesquelles le mode d'utilisation d'une ouverture de crédit pourrait échapper à la qualification de prêt (M.-D. WEINBERGER, « Funding loss... in translation », *D.B.F.*, 2014/I-II, p. 19).
**(4)** Dans un arrêt du 7 août 2013, la Cour constitutionnelle a conclu à la constitutionnalité de l'article 1097*bis* malgré la différence de traitement ainsi établie entre les emprunteurs et les bénéficiaires d'une ouverture de crédit (C. const., 7 août 2013, n° 119/2013).
**(5)** Sur le devoir qu'a le juge de qualifier adéquatement le contrat de crédit indépendamment de la qualification qui lui a été donnée par les parties, voy. notamment G.-L. BALLON, « Over de kwalificatie als lening van een kredietopening t.v.v. een onderneming - Il ne suffit pas de baptiser carpe le lapin... », *D.A.O.R.*, 2016/4, n° 120, pp.90-93 ; C. ALTER et L. VAN MUYLEM, « Article 1907*bis* du Code civil et (re)qualification de l'ouverture de crédit », *R.D.C.*, 2015/2, p. 193 ; J. CATTARUZZA, « L'indemnité de remploi au cœur des débats », *J.T.*, 2013, p. 721.
**(6)** Voy., pour les plus récentes, G.-L. BALLON, *op. cit.*, pp. 90-93 ; M.-D. WEINBERGER et E. CAPITEYN, « Le sort du crédit et le transfert de