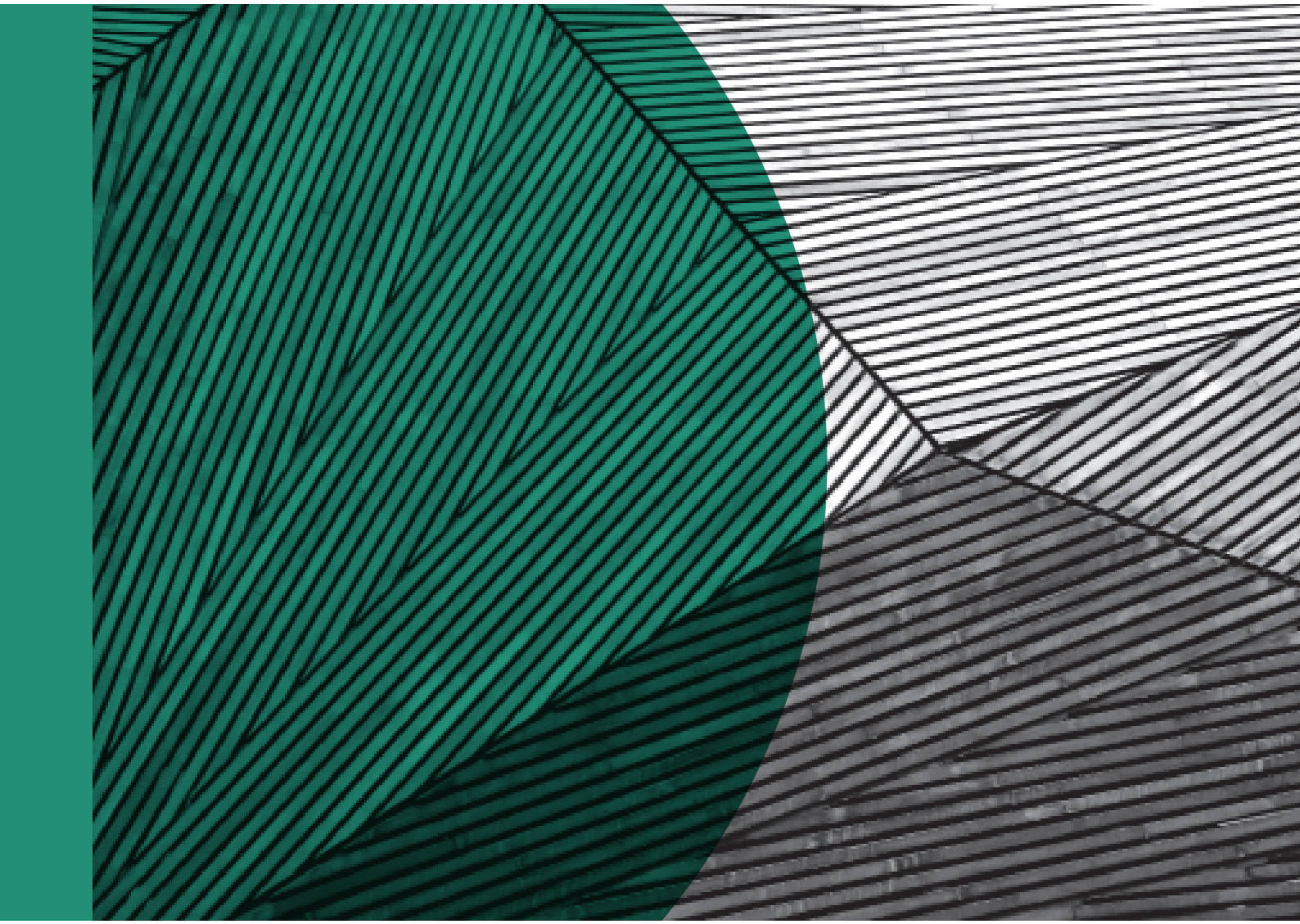
ICJP
INSTITUTO DE CIÊNCIAS JURÍDICO-POLÍTICAS
ICIDP
CENTRO DE INVESTIGAÇÃO DE DIREITO PÚBLICO

A PROTECÇÃO DE DADOS PESSOAIS NAS TELECOMUNICAÇÕES

PERSPECTIVA DA CNPD

LUÍS LIGNAU SILVEIRA



A Protecção de dados pessoais nas Telecomunicações

-perspectiva da CNPD-

I) A PROTECÇÃO DE DADOS PESSOAIS, EM GERAL

Preocupação recente e ainda não universal

A) Preocupação recente

Costuma fazer-se reportar o inicio da preocupação com a protecção de dados pessoais a um célebre artigo dos americanos Warren e Brandeis que, em 1890, propugnaram a consagração do "*right to be let alone*".

A verdade é que, nesse trabalho, o direito à protecção de dados pessoais surgia ainda dissolvido ou confundido com o direito à privacidade.

A primeira referência directa e específica à protecção de dados pessoais acabou por surgir em 1970, com a lei de protecção de dados do "*Land*" alemão do Hesse.

B) Preocupação ainda não universal

Apesar do acolhimento que tem progressivamente vindo a encontrar, sobretudo na Europa e nos países dela culturalmente mais próximos, o que é um facto é que não pode afirmar-se, com rigor, que a preocupação com a protecção de dados pessoais tenha, no presente, alcançado expansão universal.

Basta, a confirmá-lo, recordar – como o fez de resto um dos participantes em recente Conferência "*Mundial*" de protecção de dados – que a necessidade da protecção de dados não tem vindo a ser sentida em países tão populosos e importantes como a China, a Rússia e os Estados Unidos da América.

A situação na China e na Rússia explica-se, sobretudo, por motivos ideológicos (é certo que no segundo destes países terá sido aprovada legislação de protecção de dados, mas não estará em aplicação).

Nos Estados Unidos, a justificação é sobretudo de cariz económico: considera-se que os dados pessoais devem circular, para fazer funcionar o mercado (cingindo-se a legislação sobre protecção de dados a certas áreas sectoriais, como a defesa dos menores contra o abuso, nomeadamente através da Internet).

C) Expansão a nível internacional

De todo o modo, são já diversos, e relevantes, os instrumentos internacionais e comunitários directamente destinados à protecção de dados pessoais.

Para além de textos de valor recomendatório, como as Directrizes da OCDE de 1980 e as da Assembleia Geral da ONU de 1990, merece ser realçada, desde logo, a Convenção 108 do Conselho da Europa de 1981, relativa à protecção de dados tratados informaticamente.

Como Convenção que é, este texto é vinculativo, estando aberto à adesão de países membros e não membros do Conselho da Europa.

No âmbito da União Europeia, assume posição-chave a Directiva 95/46/CE do Parlamento Europeu e do Conselho, que, embora formalmente dotada dum objectivo duplo – garantir a livre circulação de dados pessoais no âmbito da União e assegurar o direito à protecção desses dados – tem vindo cada vez mais a ser entendida como a peça central de referência, a nível comunitário, para a protecção de dados pessoais.

Tanto assim é, aliás, que um dos factores que tem sido usado para aferir da democraticidade dos novos Estados pretendentes à integração é precisamente, o de constatar se eles se muniram ou não de legislação interna correspondente a transposição dessa Directiva.

Enfim, a Carta dos Direitos Fundamentais da União Europeia, inicialmente apenas dotada de eficácia recomendatória, foi incluída no Tratado de Lisboa, pelo que assumirá a relevância jurídica deste, se vier a ser ratificado por todos os Estados-Membros.

Ora, nesta Carta é expressamente consagrado o direito à protecção de dados pessoais, enquanto direito autónomo e distinto do direito à reserva da vida privada, já que ambos se encontram definidos e regulados em preceitos diversos.

D) Regulação interna

A Constituição portuguesa foi, em rigor, a primeira lei fundamental a definir e regular o direito à protecção de dados pessoais.

Como se sabe, o artigo que assim se exprimiu – artº 35º – reportava-se primeiro apenas aos dados tratados por via informática, mas, na sua versão actual, abrange também os dotados de suporte material.

Esta norma constitucional configura o cerne deste direito como a faculdade de aceder às informações relativas ao titular; aponta um regime especial para os chamados dados sensíveis; proclama a proibição de acesso a dados de terceiros, salvo permissão legal ou consentimento do próprio, e encarrega uma entidade administrativa independente de controlar a aplicação da legislação de protecção de dados.

No seguimento da disposição constitucional, e transpondo a Directiva 95/46/CE, foi emanada a actual Lei de Protecção de Dados Pessoais – Lei nº 67/98, de 26 de Outubro.

E) **Princípios e direitos básicos da protecção de dados pessoais**

A Lei nº 67/98, em consonância com os instrumentos internacionais e comunitários aplicáveis, define uma série de princípios e direitos essenciais em matéria de protecção de dados pessoais.

1) **Princípios básicos**

De entre os princípios básicos relativos à protecção de dados pessoais, cabe salientar:

a) Princípio da finalidade

Os dados pessoais não podem ser utilizados para finalidades incompatíveis com as que justificaram a sua recolha.

Foi por esta razão, p.e., que a CNPD recusou que a Ordem dos Advogados cedesse a lista dos seus associados a uma empresa que pretendia utilizá-la para fins de "*marketing*".

b) Princípio da proporcionalidade

Os dados pessoais devem ser tratados por forma adequada e não excessiva, guardando a justa medida entre a satisfação dos interesses que levaram à sua recolha e a salvaguarda da privacidade dos titulares.

Foi fazendo apelo a este princípio que a CNPD, p.e., não admitiu que o tratamento de dados de juízes, a cargo do Conselho Superior da Magistratura, incluísse os nomes dos respectivos cônjuges.

c) Direito ao esquecimento

Os dados pessoais não devem ser guardados por tempo indefinido

Apenas devem poder ser tratados e conservados pelo período correspondente à consecução das finalidades para que foram recolhidos.

Por isso a Lei nº 67/98 incumbe a CNPD de fixar esse prazo máximo de utilização

Apenas em casos excepcionalíssimos e devidamente justificados tem a CNPD aceite que tal conservação se faça por tempo indeterminado.

d) Minimização

Se a informação significa poder, daí decorre que possuir informações respeitantes a outras pessoas se traduz sempre numa forma de deter poder sobre elas.

Por isso se vem cada vez mais insistindo na importância da "*minimização*" dos dados pessoais – ou seja, na desejabilidade do tratamento de dados pessoais em escala tão reduzida quanto possível.

2) Direitos fundamentais

O chamado direito à protecção de dados pessoais consiste, afinal, num conjunto de direitos a estes respeitantes – dos quais os mais relevantes são o direito de informação e o direito de acesso.

a) Direito de informação

O primeiro e básico direito dos titulares de dados pessoais é o de informação – ou seja, o de ser informado de que dados pessoais seus estão a ser tratados, por quem, com que finalidade.

A relevância deste direito é particularmente "*visível*", p.e., no que respeita ao tratamento de dados por videovigilância, em que se impõe que o responsável afixe avisos a publicitar a captação de tais imagens, qual a respectiva finalidade e quem assim procede.

b) Direito de acesso e rectificação

A Lei Fundamental aponta no sentido de que o cerne da protecção de dados reside no direito de a estes aceder, para se verificar se os mesmos estão correctos e actualizados.

O direito de informação representa, sobretudo, um instrumento para o bom exercício deste direito de acesso.

Corolário lógico deste direito de acesso é o de rectificar e actualizar os dados que se tenha constatado estarem incorrectos ou desactualizados.

Situação em que não raras vezes este direito ganha relevância é a do acesso a dados dos tratamentos a cargo das polícias.

Como os tribunais não estão (infelizmente) obrigados a enviar às polícias informação acerca das decisões finais proferidas, não é raro que figurem ainda em tratamentos de dados policiais pessoas que, a final, vieram a ser absolvidas.

II) A PROTECÇÃO DE DADOS NAS TELECOMUNICAÇÕES

A) Principais instrumentos

Presentemente, vigora a respeito das comunicações electrónicas a Directiva 2002/58/CE, de 12 de Julho de 2002, transposta para a ordem interna portuguesa pela Lei nº 41/2004, de 18 de Agosto de 2004.

Esta Directiva teve em mira aplicar, à área das comunicações electrónicas, os princípios gerais de protecção de dados definidos na Directiva 95/46/CE.

Apesar de relativamente recente, não deixou já de ser objecto de algumas críticas, nomeadamente no tocante ao seu âmbito: tem-se afirmado, com efeito (embora essa perspectiva não acolha geral aceitação), que é demasiado restrito o alcance da Directiva, ao cingir-se às comunicações "*externas*", sem abranger também as comunicações que ocorrem dentro de cada instituição.

E está já em curso um procedimento de modificação parcial deste instrumento, tendente a reforçar as medidas de segurança aplicáveis, e, porventura, a repensar a própria noção de "*dado pessoal*".

Entretanto, verificou-se uma alteração da Directiva em causa – através da Directiva 2006/24/CE, de 15 de Março de 2006.

B) Dados pessoais relevantes

1) Dados de conteúdo

A CNPD tem sustentado a posição – aliás generalizada entre as suas congéneres – de que os dados de conteúdo das comunicações electrónicas estão sujeitos ao regime geral do sigilo das comunicações.

Tem-lhe merecido especial atenção, nesta perspectiva, o tratamento consistente na comunicação de dados de saúde através da Telemedicina.

Embora não exista (ainda) qualquer deliberação geral da CNPD acerca desta matéria, pode deduzir-se das autorizações concedidas que:

a) Se considera que a telemedicina envolve o tratamento de dados pessoais (se se reportar a pessoas identificadas ou identificáveis).
b) Embora estejam em causa dados sensíveis – dados de saúde – o seu tratamento não precisa, para se legitimar, do consentimento expresso dos titulares, pois pode apoiar-se em norma legal precisa: o artigo 7º, nº 4 da Lei nº 67/98, enquanto admite o tratamento de dados de saúde no âmbito do diagnóstico e prestação de cuidados de saúde, na medida em que o tratamento seja realizado por profissionais sujeitos a sigilo profissional.
c) Ressalvadas as situações de urgência, aos titulares dos dados devem ser reconhecidos os direitos de informação e de acesso acerca dos tratamentos.
d) O tratamento deve estar garantido por rigorosa confidencialidade (dentro, claro, do âmbito justificado pelo adequado acompanhamento médico, que pode não ser individualizado, mas abranger toda uma equipa médica).

2) <u>Dados de tráfego</u>

Perante a Directiva 2002/58/CE, é hoje indubitável que os dados de tráfego – relativos ao emitente e ao receptor, ao meio, data, ocasião e duração da comunicação – constituem dados pessoais, desde que concernentes a pessoas singulares identificadas ou identificáveis.

Eles deverão mesmo, na ordem jurídica portuguesa, ser considerados dados sensíveis, já que relativos à "*vida privada*".

É certo que o artigo 8º da Directiva 95/46/CE não inclui os dados da "*vida privada*" no elenco de dados sensíveis que enuncia.

Mas a ordem jurídica portuguesa tem uma concepção mais ampla de dados sensíveis, pois neles integra os respeitantes à vida privada – artº 35º, nº 3 da Constituição e artº 7º, nºs 1 e 2 da Lei 67/98.

Apesar de por vezes ter sido posta em causa esta opção do legislador português – mesmo por banda de alguns representantes autorizados da Comissão Europeia – a verdade é que a enumeração da Directiva não deverá ser qualificada de taxativa, mas tão-somente como representando um elenco mínimo.

E, ademais, a Constituição portuguesa deve – a nosso ver – ser entendida como possuindo nível vinculativo superior às regras de Direito Comunitário.

3) <u>A emissão</u>

No concernente à emissão de comunicações electrónicas vigora, como princípio geral, o da liberdade – enquanto expressão da genérica liberdade de expressão do pensamento.

Não deixa, porém, de suscitar-se a este propósito a questão da aplicabilidade de tal perspectiva aos menores.

Formalmente, pareceria que o entendimento de que estes seriam incapazes de exercício de direitos, nessa medida suprida pelos seus representantes, conduziria à conclusão de que a liberdade de emissão de comunicações deveria ter-se por condicionada, assim, pelo instituto da representação.

Esta visão formalista não pode ajustar-se à realidade, havendo que reconhecer que os menores atravessam, até atingir os 18 anos, vários graus de progressivamente mais sólida maturidade, que já lhes permitirão emitir comunicações (electrónicas e outras) com suficiente consciência de tal procedimento.

A outra conclusão não poderia deixar de conduzir – mesmo no caso de inexistência de legislação interna que reconheça tal graduação de capacidade – o disposto no artº 27º da Convenção das NU sobre os Direitos da Criança, que a esta reconhece expressamente o direito ao desenvolvimento.

4) <u>A recepção</u>

A recepção de comunicações é também regida pelo princípio da liberdade, aqui enquanto manifestação da mais ampla liberdade de informação.

A Directiva 2002/58/CE instituiu, a este respeito – inovadoramente – a regra de "*opt-in*", segundo a qual a recepção de comunicações electrónicas está sujeita ao prévio consentimento do destinatário.

Pretendeu-se, assim – após viva e aprofundada discussão durante a preparação da Directiva – poupar o destinatário ao esforço e dispêndio que a recusa da comunicação recebida sempre envolveria.

a) <u>Marketing político</u>

A CNPD já teve oportunidade de tomar posição acerca da aplicação da regra de "o*pt-in*" ao "*marketing*" político através de "*e.mail*".

Constatou, com efeito, que a maioria dos partidos políticos não estava ciente desse regime, tendo vários remetido "*marketing*" político através de "*e.mail*" sem prévia solicitação dos interessados.

Emitiu, por isso, uma deliberação geral (nº 143/2002, de 9 de Julho de 2002) esclarecendo que esse procedimento dependeria sempre de prévio consentimento dos destinatários.

Precisou, a propósito, que nem seria legítimo enviar "*e.mail*" a perguntar se os destinatários pretenderiam receber esse tipo de comunicações: é que mesmo essa pergunta já teria de obedecer ao princípio do "*opt-in*".

O eventual questionamento sobre o desejo de receber propaganda política por essa via teria de realizar-se por meio não personalizado: anúncio público; comunicação social; cartazes.

b) Comunicações não solicitadas, em geral

Aferindo segundo a mesma perspectiva a generalidade das comunicações por via electrónica não solicitadas, a CNPD tem intervindo quando lhe são apresentadas queixas a tal respeito, aplicando coimas e procurando obstar à repetição de tais procedimentos.

Esta intervenção é, contudo, sempre muito problemática quando se está perante verdadeiro "*spam*" – envio massivo de mensagens, normalmente com fins publicitários.

É sabido que, no campo dos princípios, se tem confrontado a perspectiva que considera irregular tal actuação, com a que a admite, com base no respeito da liberdade de expressão.

Mas os prejuízos que o "*spam*" tem acarretado, para o bom funcionamento do sistema de comunicações em geral, e para a privacidade dos seus destinatários, tem justificado que contra ele se reaja, a nível nacional e internacional.

A CNPD tem podido intervir nos contados casos em que consegue identificar a origem desse tipo de mensagens, e quando ela se situa no âmbito da sua competência geográfica e legal.

Há que reconhecer, contudo, que em muitas situações assim não sucede – verificando-se que a maioria das acções de "*spam*" tem origem, directa ou indirecta, nos EUA e em vários países asiáticos.

Algumas tentativas de obstar a tal problema – como a da "*boîte à spam*" ensaiada pela CNIL francesa – não têm tido o desejado resultado.

Apenas uma acção concertada a nível internacional poderá porventura contribuir para o controlo deste fenómeno.

5) O controlo

a) Controlo de dados de conteúdo

Os dados de conteúdo das comunicações electrónicas (e das demais) só devem poder ser acedidos por terceiros à relação emitente – destinatário com base em lei, em decisão judicial ou no consentimento dos interessados.

A CNPD tem tido oportunidade de vincar este entendimento em diversas áreas da sua competência.

Tem-no feito, designadamente, a propósito dos – crescentes – exemplos de "*call-centers*" de empresas que tem autorizado.

Só tem emitido autorizações, nesses casos, desde que os clientes que telefonam para tais "*call-centers*" sejam logo de início avisados de que as suas chamadas vão ser gravadas e hajam depois manifestado por modo expresso que consentem nessa gravação.

Por seu turno, os trabalhadores afectos aos "*call-centers*" terão também de ter consentido na gravação das chamadas que atendem – devendo ser-lhes distribuído tarefa diferente se não o fizerem.

Isto vale, naturalmente, com ressalva daquelas hipóteses – comprovação de negociações ou celebração de contratos; recurso a serviços de urgência – em que a própria lei (Lei nº 41/2004, de 18 de Agosto, artº 4º, nº 4) admite sem mais tal gravação.

Por seu turno, na Deliberação geral de 29 de Outubro de 2002, sobre controlo das comunicações dos trabalhadores no local de trabalho, a CNPD apenas considerou possível, a título muito excepcional, o acesso dos empregadores ao conteúdo de "*e-mails*" recebidos pelos trabalhadores que se encontrem doentes ou em gozo de férias.

b) Controlo de dados de tráfego

Na já citada Deliberação de 21 de Outubro de 2002, a CNPD explanou os critérios que recomenda às entidades patronais que pretendem controlar os dados de tráfego de comunicações realizadas pelos seus trabalhadores em período laboral.

Sugeriu, assim, que se comece sempre por uma abordagem geral dessas comunicações, e, depois, se necessário, discriminada por sectores.

A revelar-se absolutamente necessária uma verificação em relação às comunicações de certo trabalhador, propôs-se que ela se fizesse na presença do próprio e/ou na de um representante dos trabalhadores.

6) Retenção de dados

A retenção ou conservação de dados de tráfego respeitantes às telecomunicações pode, naturalmente, ter diversos objectivos que merecem ser considerados, nomeadamente para efeitos de prova.

Mas contrapõe-se ao legítimo interesse dos titulares dos dados em que estes não sejam tratados por tempo indefinido.

É por isso que a Directiva 2002/58/CE estabeleceu, como regra básica, a de que os dados de tráfego relativos à comunicação devem ser destruídos uma vez esta concluída, salvo um período de seis meses de conservação para efeitos de facturação (artº 6º).

É sem dúvida relevante considerar que a Directiva 2006/24/CE, de 15 de Março de 2006, veio alterar este regime, permitindo, em relação à investigação de crimes graves, a conservação de dados de tráfego entre seis meses a dois anos.

O originário projecto de proposta de lei de transposição desta Directiva, submetido a parecer da CNPD, apontava para o período máximo, de dois anos.

No seu parecer (nº 38/2007, de 16 Julho de 2007) a CNPD pronunciou-se no sentido de esse período, embora contido nos limites da Directiva, ser excessivo; além de preconizar a definição mais rigorosa dos crimes cuja investigação justificará o acesso a tais dados nesse período.

Estas sugestões da Comissão vieram a ser acolhidas no texto da proposta de lei apresentada à Assembleia da República.

Nota final

Como nota final, merece realçar-se a constante e cada vez mais célere evolução tecnológica que tem beneficiado as telecomunicações.

O Direito procura acompanhar essa evolução, mas normalmente só o consegue com certo desfasamento e atraso.

Luís Lingnau da Silveira

amm