

BOLETIM
irib

EM REVISTA
ESPECIAL

Nº 361
Junho 2020

ISSN 1677-437X
Publicação do
Instituto de Registro
Imobiliário do Brasil



A LEI GERAL DE PROTEÇÃO DE DADOS EM DEBATE

Proteção de Dados Pessoais e os Registros Públicos



Sumário

- 3 Editorial**
- 4 Apresentação**
FRANCISCO LOUREIRO
- 6 Novas tecnologias e os impactos causados nas formas de viver em sociedade**
GERALDO FRANCISCO PINHEIRO FRANCO
- 14 O Impacto das Novas Tecnologias nos Registros Públicos**
ANTONIO CARLOS ALVES BRAGA JÚNIOR
- 26 Panorama atual do Regulamento Europeu sobre a Proteção de Dados (RGPD) e os Registros Públicos. Desafios e perspectivas**
MADALENA TEIXEIRA
- 42 A proteção registral de dados pessoais e sistemas registraes europeus. Medidas práticas – a experiência portuguesa e europeia**
SOLANO DE CAMARGO
- 52 Lei Geral de Proteção de Dados – uma aproximação aos conceitos da lei**
BRUNO RICARDO BIONI
- 64 O Poder Público na LGPD – regime jurídico aplicável aos serviços notariais e de registros**
FERNANDO ANTONIO TASSO
- 76 Princípio de divulgação com rogação em xequê. Legitimidade para postular a produção da publicidade registral em suas várias modalidades**
CALEB MATHEUS RIBEIRO DE MIRANDA
- 92 Ontologia registral – sujeitos de direito e suas representações nos Registros Públicos**
IVAN JACOPETTI DO LAGO
- 104 Ontologia registral – Sujeitos de direito e suas representações nos Registros Públicos**
MARCELO SALAROLI
- 116 Direito ao esquecimento e os Registros Públicos**
CINTIA ROSA PEREIRA DE LIMA
- 128 A publicidade jurídico-registral, seu objeto e veículo de sua difusão**
RAFAEL RICARDO GRUBER
- 136 A publicidade jurídico-registral, seu objeto e veículo de sua difusão**
JULIANO MARANHÃO
- 146 Boas práticas e governança no tratamento de dados registraes**
CLAUDIO MACHADO
- 154 Boas práticas e governança no tratamento de dados registraes**
ADRIANA JACOTO UNGER
- 160 Direito à informação x publicidade registral**
LUÍS PAULO ALIENDE RIBEIRO
- 168 Homenagem | LUIZ CARLOS ANDRIGHETTI**

LGPD e os novos desafios lançados aos Serviços Extrajudiciais

O Instituto de Registro Imobiliário do Brasil (IRIB) e a Associação dos Registradores de Pessoas Naturais do Estado de São Paulo (Arpen/SP), em parceria com a Escola Paulista da Magistratura (EPM), realizaram, nos dias 2 e 3 de setembro de 2019, na sede da EPM, o seminário **A Lei Geral de Proteção de Dados em debate – Proteção de Dados e os Registros Públicos**. O evento contou com a coordenação dos desembargadores Marcelo Martins Berthe e Luís Soares de Mello Neto e dos juízes Antonio Carlos Alves Braga Júnior e Fernando Antonio Tasso.

A abertura do evento ficou a cargo do Corregedor-Geral da Justiça do Tribunal de Justiça de São Paulo, desembargador Geraldo Francisco Pinheiro Franco, que destacou sua preocupação em relação às grandes responsabilidades trazidas pela Lei Geral de Proteção de Dados tanto para o judicial quanto para o extrajudicial. “A adequação dos direitos individuais das pessoas com os interesses dos agentes econômicos, imobiliários, do mercado em geral, e especialmente dos que atuam na obtenção e no tratamento dos dados, é o desafio lançado a todos nós, agentes do Poder Público e dos Serviços Extrajudiciais”, lembrou.

O programa incluiu temas como o impacto das novas tecnologias nos Registros Públicos, uma análise do Regulamento Europeu sobre a Proteção de Dados (GDPR) nos Registros Públicos e o estudo do conteúdo da LGPD: seus conceitos, regime jurídico aplicável aos registradores, direito à informação *versus* publicidade registral, direito ao esquecimento, boas práticas e governança no tratamento de dados registrares etc.

Esta edição do *Boletim do IRIB em revista* é inteiramente dedicado a esse debate da Lei nº 13.709/2018 – Lei Geral de Proteção de Dados (LGPD), que brevemente entrará em vigor, e que contou com juristas, registradores e outros especialistas no tema.



SÉRGIO JACOMINO
Presidente do IRIB

LGPD: conteúdo, contornos e limites

Fiquei profundamente honrado pelo convite que me foi feito, de apresentar esta obra coletiva que reúne textos que condensam as palestras e os debates travados durante o curso **A Lei Geral de Proteção de Dados em debate – proteção de dados e os Registros Públicos**, ministrado nas dependências da Escola Paulista da Magistratura nos dias 2 e 3 de setembro de 2019.

Na qualidade de Diretor da Escola Paulista da Magistratura (biênio 2018/2019), foi com satisfação que recebi durante dois dias os palestrantes e os debatedores de tema novo e desafiador, que despertou o interesse de dezenas de magistrados, notários, registradores e demais profissionais do direito.

Contou o evento com o apoio da Corregedoria Geral da Justiça, do Instituto de Registro Imobiliário do Brasil (IRIB) e da Associação dos Registradores de Pessoas Naturais do Estado de São Paulo (Arpen-SP).

O envolvimento pessoal do então Desembargador Corregedor Geral da Justiça Geraldo Francisco Pinheiro Franco – hoje Presidente do Tribunal – e de sua equipe de juízes assessores foi fundamental para o sucesso do evento.

A coordenação do curso ficou a cargo do Desembargador Marcelo Martins Berthe e dos Juízes Antonio Carlos Alves Braga Júnior e Fernando Antonio Tasso, a quem agradeço toda a colaboração prestada ao longo do biênio que estive à frente da EPM.

Não posso deixar de agradecer a colaboração decisiva do Desembargador Luís Soares de Mello Neto, coordenador da área de Tecnologia da Informação e Direito Digital da EPM – hoje vice-Presidente do Tribunal de Justiça – não somente pelo apoio ao seminário, como também pela intensa atividade acadêmica durante todo o biênio de 2018/2019.

Participaram ativamente da montagem e da execução do seminário o IRIB, por seu presidente registrador Sérgio Jacomino e a Arpen-SP, por suas registradoras Daniela Silva Mroz e Karine Maria Famer Rocha Boselli, a quem também agradeço pelo empenho e comprometimento.

A Lei Geral de Proteção de Dados (Lei 13.709/2018) é ainda uma grande desconhecida. O período de *vacatio legis* breve se escoará, de modo que se torna premente conhecer o conteúdo, contornos e os limites dos dados que podem ou não ser divulgados.

A situação é mais difícil no que se refere ao Poder Público e aos serviços delegados de Notas e de Registro. Isso porque se preordenam mencionados serviços a conferir segurança jurídica mediante – entre outros instrumentos – a publicidade dos atos que praticam e dos dados que se encontram em seus arquivos.

A vocação do Notariado e do Registro é publicizar. Muitos dos efeitos dos direitos inscritos se subordinam ou estão estritamente ligados à publicidade.

Tome-se como exemplo a natureza constitutiva do registro imobiliário em relação à transmissão ou oneração de bens imóveis. O absolutismo dos direitos reais, sua principal característica, da qual decorrem todas as demais, se encontra intimamente ligado à publicidade, entendida como a possibilidade de terceiros conhecerem ou poderem conhecer a titularidade e a extensão dos direitos reais alheios. Não se concebe o efeito *erga omnes* dos direitos reais separado do sistema publicitário do registro imobiliário.

Também o estado das pessoas naturais é dotado de absolutismo, de modo que aos registradores civis competirá a sofisticada tarefa de separar dados que devem dos dados que não podem ser publicizados.

É nesse contexto que o intérprete terá a delicada missão de separar quais são os dados sensíveis dos titulares dos direitos, que não podem ser divulgados, pena de responsabilização civil, daqueles que não somente podem, mas devem ser divulgados, para que as atividades Notarial e de Registro cumpram a sua função.

A tarefa não é fácil e exigirá disciplina permanente de todos os atores, porque contrária à longa tradição de publicidade a que se preordena a atividade registral e notarial. Haverá quase um exercício diário de controle de hábitos, para que dados que sempre foram públicos deixem de sê-lo, sem prejuízo à própria finalidade dos serviços.

Não há dúvida de que a LGPD se fazia necessária, com o propósito de proteger interesses de estatura constitucional – privacidade e intimidade. Seguiu a melhor experiência, inspirando-se na legislação da Comunidade Europeia.


Certamente haverá necessidade da edição de normas de regência por parte da Corregedoria Geral da Justiça e do Conselho Nacional de Justiça, uma vez que não desce e lei a detalhes – e não poderia – de aspectos das atividades notariais e registrares.

Essa a razão de o seminário e os trabalhos, que ora se publicam e condensam o que ali foi discutido, serem multidisciplinares. Participaram juízes, notários, registradores, advogados e profissionais da área digital, todos empenhados em delimitar quais dados poderão ser divulgados e quais as ferramentas hábeis a tal função.

Boa leitura a todos, com a certeza de que a obra não apenas será útil, mas fundamental diante da cada vez mais próxima vigência da lei.

FRANCISCO LOUREIRO
Desembargador do TJSP





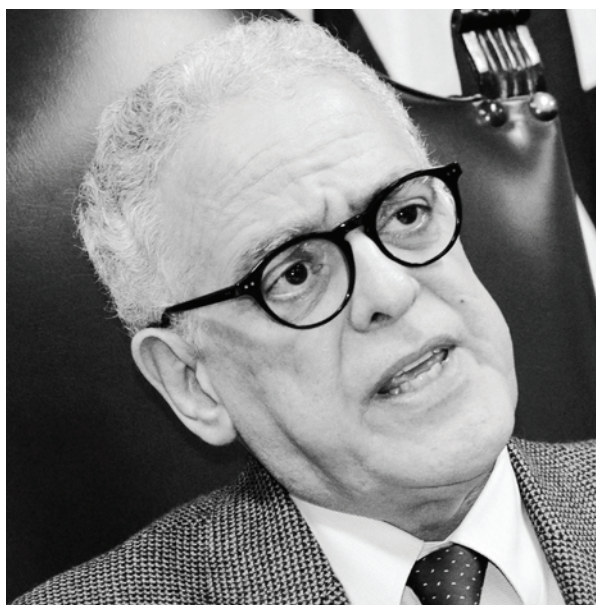
**Novas
tecnologias
e os impactos
causados
nas formas
de viver em
sociedade**

**Novas
tecnologias
e os impactos
causados
nas formas
de viver em
sociedade**

Novas tecnologias e os impactos causados nas formas de viver em sociedade



Agradeço a gentileza do convite para a



**DESEMBARGADOR GERALDO FRANCISCO
PINHEIRO FRANCO**
Corregedor-Geral da Justiça do Estado de São Paulo

abertura deste seminário, que diz respeito à Lei Geral de Proteção de Dados, e o vínculo, não só com a área judicial, mas com a área extrajudicial. Nós temos uma preocupação muito grande porque a lei está em vias de entrar em vigor e as responsabilidades decorrentes são muito amplas e muito sérias para todos nós.

Precisamos debater exaustivamente esse tema para saber, objetivamente, o que nós podemos e o que não podemos fazer e até onde é possível tratar com dados de terceiros.

Essa iniciativa da Escola Paulista da Magistratura – e a EPM tem sido pioneira nesses debates – é de uma importância capital. Vou fazer brevemente observações muito objetivas, e eu quero, antes de mais nada, agradecer ao desembargador Loureiro, e aos desembargadores Cortez, Luís Soares e Marcelo Berthe, Fernando Tasso e Alves Braga, que são eles sim profissionais de conhecimento, a gentileza do convite. Um deles é que devia estar abrindo o evento, mas por delicadeza é que me confiaram esta oportunidade.

Tutela de direitos das pessoas reconhecidos como fundamentais

Vou começar dizendo que novas tecnologias propiciam novas formas de geração e de circulação de riqueza, mas não asseguram sua distribuição de forma equânime, nem a proteção das pessoas envolvidas nos sistemas produtivos ou atingidas pelos impactos causados nas formas de viver em sociedade.

Assim ocorreu com a revolução agrícola, com a retomada das relações comerciais a partir do final da Idade Média, com a revolução industrial e, mais recentemente, com a informatização em larga escala que determinou a formação da atual sociedade da informação.

Essa informatização em larga escala, agora aplicada à obtenção e tratamento de dados pessoais, novamente coloca os órgãos do Poder Judiciário e os delegatários dos serviços extrajudiciais como agentes da produção e circulação de riqueza e como responsáveis pela tutela de direitos das pessoas reconhecidos como fundamentais.

Abro um parêntese para lembrar que as restrições impostas pela legislação têm direta vinculação com os

direitos ditos fundamentais. E nossa preocupação é que o Poder Judiciário – e quando digo Poder Judiciário eu faço referência ampla, seja na atuação jurisdicional, na atuação administrativa, e na atuação vinculada às delegações – tem que estar preparado para prestar não só excelente serviço, mas para, no seu objetivo final, transmitir segurança aos interessados. E segurança inclusive na preservação dos direitos nem sempre vinculados ao ato em si. Daí a importância dos debates que hoje se iniciam.

Nessa perspectiva, o desenvolvimento e a disseminação das tecnologias que permitem o tratamento de dados pessoais obtidos em larga escala, através de diferentes formas de relacionamentos interpessoais, devem encontrar, no Poder Público, e nos Serviços Extrajudiciais, o anteparo dos direitos pessoais, e ao mesmo tempo, o incentivo a que a riqueza assim gerada beneficie os agentes econômicos, o mercado e a sociedade em seu todo.

A proteção dos dados pessoais encerra concretização da garantia e promoção da dignidade da pessoa frente às várias possibilidades de violação da intimidade e mesmo da própria condição humana.

A garantia da liberdade e da privacidade das pessoas também passa pela possibilidade de conhecimento e anuência quanto ao uso dos dados pessoais.

Nessa perspectiva a proteção concedida pela Lei Geral de Proteção de Dados, em última análise, é a tutela do ser humano.

Os serviços notariais e de registro são, em sua essência, depositários de dados pessoais e econômicos confiáveis.

A obtenção desses dados é compulsória em relação aos seus titulares, mas seu acesso por terceiros é livre diante do art. 16 da Lei nº 6.015/1973.

A liberdade de acesso, porém, foi concebida na forma de fornecimento de certidões, que antes da disseminação do uso dos computadores eram solicitadas pessoalmente no balcão do cartório e lavradas de forma manual, quan-

do muito com uso de formulários e máquinas de escrever.

Esses dados, porém, migraram dos livros físicos para o mundo digital, integrando arquivos eletrônicos que podem ser acessados e manipulados com o uso de programas de informática que a cada dia se tornam mais rápidos, eficazes, baratos e de fácil aquisição.

A concentração dos dados em arquivos eletrônicos, mantidos sob a responsabilidade dos notários e registradores, alia-se às novas formas de acesso pelos usuários em geral que, à distância e por vezes utilizando “robôs” (ou programas informatizados), demandam diretamente das serventias, ou por meio de Centrais Eletrônicas, o fornecimento de dados que podem ser utilizados para as mais diversas finalidades, lícitas ou não.

E aqui eu lembro um caso concreto que nós tivemos há pouquíssimo tempo na Corregedoria, em que um determinado cidadão lavrou uma partilha junto a um tabelionato e posteriormente veio à Corregedoria pleitear que aqueles dados lançados na partilha, embora públicos pela sua essência, e que não tinham inclusive interesse terceiro, mas pela expressão de vulto do pa-

trimônio daquele interessado, não fossem transmitidos em forma de certidão para ninguém porque isso poderia causar danos de ordem de segurança, danos de ordem pessoal, danos de ordem patrimonial e, por decisão da Corregedoria, nós entendemos que esse cidadão tinha absoluta razão no que pleiteou. Embora um ato público dirigido a quem quiser ter acesso a ele, para qualquer fim, pudesse, em tese, ser objeto de uma certidão, nós entendemos, pelas situações e pelas ponderações concretas, que ele não devesse ser transmitido, salvo com autorização judicial, para fins de prova ou para outros fins específicos.

Esse é um exemplo concreto de limitação de um ato público dirigido a todos e que o Estado há de preservar o interesse dos participantes dele.

Responsáveis pelos serviços extrajudiciais devem atuar como protetores dos titulares dos dados pessoais

Nesse ponto os agentes públicos e os responsáveis pelos serviços extrajudiciais devem atuar como protetores



dos titulares dos dados pessoais, agindo para que sua obtenção, tratamento e posterior divulgação, de forma total ou parcial, não viole direitos fundamentais dos titulares desses dados que são as pessoas naturais a que eles se referem.

Desse modo, independentemente de quem os obtém, arquiva, trata e divulga, a primeira tutela a ser concedida é às pessoas titulares dos dados, tenham ou não valor econômico aquilatável individualmente, ou valor agregado, quando unidos aos dados de igual natureza obtidos em relação a outras pessoas.

Como exemplo, além desse caso concreto que nós tivemos, não é difícil imaginar os danos que a divulgação de dados de pessoas identificadas pode causar quando se referirem ao gênero indicado no assento de nascimento e às suas eventuais alterações, para adequação à identidade sexual, ainda que assim ocorra para o incremento da atuação de empresas voltadas ao atendimento de demandas de públicos específicos.

É preciso ter isso bem claro, e a necessidade de uma mudança de cultura do que nós entendemos ser um dado

público com restrição objeto da Lei. É possível que um indivíduo que tenha anotações registraes relativas a gênero, por exemplo, não queira, por razões eminentemente pessoais, que essas informações sejam transferidas ou transmitidas a todos.

É uma questão muito própria, e que nós precisamos entender, ou reentender os alcances e as consequências da violação dessas informações, do resguardo dessas informações. A matéria não é leve, não é clara, não é objetiva, e talvez tenha muito de subjetiva, e é isso, exatamente isso, que nós temos que debater.

O que fazer com informações que, a um primeiro momento, não revelem maiores consequências, mas que, no subjetivismo de alguém, essas informações podem gerar dano, podem gerar dano à sua intimidade, podem gerar violação ao patrimônio e, enfim, com as consequências daí decorrentes, consequências essas que são muito sérias?

Também não se encontra dificuldade em aquilatar os riscos à segurança quando a informação de todo o patrimônio imobiliário de uma pessoa pode ser obtida



“Compete-nos a discussão aprofundada para o cumprimento dos mandamentos da LGPD, possibilitando as escolhas adequadas para proteção e realização da condição humana diante das profundas modificações sociais provadas pela evolução, senão revolução tecnológica.”

mediante busca automatizada, sem identificação segura de quem a promoveu, ou com a divulgação do resultado de maneira indiscriminada. Então é uma outra questão. Alguém pode querer informações de um cidadão, seja ele quem for, em qualquer circunstância, e por intermédio do uso da rede, nem sempre se identificando efetivamente, ou às vezes apresentando uma falsa identificação, e obter dados que não lhe dizem respeito, ou lhe dizem respeito para o mal, ou dados que, a rigor, são privilegiados e que só poderiam ser obtidos por outras vias que não esse alcance direto. Essa é mais uma questão que nós certamente vamos debater e divagar neste seminário.

No lado oposto, é fácil constatar os benefícios que a obtenção de dados seguros sobre a quantidade de nascimentos em determinada área e as idades das genitoras podem proporcionar ao Estado na formulação de suas políticas públicas de saúde, assistência social e educação.

Os dados econômicos dos Registros de Imóveis, por seu lado, possibilitam a formação de indicadores seguros para o mercado imobiliário e financeiro que são grandes fontes de geração e circulação de riqueza.

E aí eu fico imaginando, e é uma reflexão que eu faço internamente, da efetiva necessidade de nós chegarmos a um denominador comum, porque não se pode instaurar o pânico a partir dessa lei, que é uma lei importante. Na medida em que todos os dados que nós imaginarmos, no âmbito do Poder Público e no âmbito das delegações, que estão cobertos pela lei, nós chegamos a uma preocupação, a uma geração de pânico, que pode inclusive emperrar a atividade de todos nós.

LGPD não pode impossibilitar o cidadão de exercer seus direitos nem emperrar a atividade do Estado

Nós temos que discutir, nós temos que compreender a Lei Geral de Proteção de Dados como uma legislação em

defesa do cidadão, mas uma legislação que não impossibilite o cidadão de exercer suas atividades, seus direitos, e muito menos – nesse caso de obtenção de dados junto aos Registros de Imóveis ou junto aos Registros Cíveis – que inviabilize o próprio Estado à prática de ações voltadas a implementar a economia, a implementar políticas de saúde, de tal sorte que a legislação venha a emperrar a atividade do Estado.

Não. Não é essa a ideia. Como deva ser esse limite, eu confesso que ainda não tenho nenhuma ideia concreta. Isso só o tempo é que vai nos levar a um denominador. Muito debate, muita reflexão, muita serenidade, muita ponderação, que vão nos levar a chegar a um ponto médio de proteção, sem a preocupação e emperramento de todo um trabalho de gente muito séria, seja no âmbito judicial, seja no âmbito extrajudicial.

Desse modo, o acesso aos dados pessoais armazenados nas serventias extrajudiciais envolve tanto a possibilidade da promoção dos direitos humanos e da cidadania das pessoas, como pode acarretar grave ofensa a esses mesmos direitos.

Compete-nos a discussão aprofundada dessas questões para o cumprimento dos mandamentos da LGPD, possibilitando as escolhas adequadas para proteção e realização da condição humana diante das profundas modificações sociais provadas pela evolução, senão revolução tecnológica.

Os seres humanos há muitos séculos conhecem e dominam a técnica, a exemplo do plantio agrícola e a criação de animais, todavia, a tecnologia não permite conhecimento amplo e tampouco seu controle no sentido de evitar possíveis danos.

A adequação dos direitos individuais das pessoas com os interesses dos agentes econômicos, imobiliários, do mercado em geral, e especialmente dos que atuam na obtenção e no tratamento dos dados, é o desafio lançado

a todos nós, agentes do Poder Público e dos Serviços Extrajudiciais.

Esse desafio deve mirar e obedecer aos mandamentos constitucionais concernentes à construção de uma sociedade livre, justa e solidária, garantir o desenvolvimento nacional, erradicar a pobreza e a marginalização e reduzir as desigualdades sociais e regionais, promovendo o bem de todos, como previsto no artigo 3º da Constituição Federal.

Os estudos aprofundados sobre o tema são, neste momento, o primeiro e importante passo para a obtenção de soluções satisfatórias que estejam em compasso com a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) cuja vigência se aproxima rapidamente.

Para isso, entre outras iniciativas, foi constituído Grupo de Estudos conjunto da Corregedoria Geral da Justiça com a Escola Paulista da Magistratura, visando propor soluções para a aplicação da Lei Geral de Proteção de Dados nos âmbitos de atuação administrativa do Poder Judiciário.

E aí eu volto a insistir: as dúvidas são muitas. Se de um lado a lei exige no campo do direito público a plena publicidade de atos, agora vem uma nova lei que não revogou, evidentemente, nessa parte da Lei Geral, as normas, inclusive de natureza constitucional, e diz que se houver extrapolação no fornecimento de dados, nós podemos ser responsabilizados por isso.

Então, esse balanceamento é difícil. Eu não imagino exatamente como nós vamos, a curto prazo, chegar a uma definição sobre isso. Mas nós temos que chegar. E o caminho é debater mesmo, não há outra solução.

Eu também queria dizer que, além dessa preocupação junto à Escola, eu também, como tenho feito sempre, me aproximei das entidades de notários e registradores, solicitando a contribuição para que a normatização em relação aos serviços extrajudiciais, frente à oportuna aplicação da Lei Geral, seja ampla e eficaz, atingindo-se, desse modo, a finalidade de sua edição.

E com satisfação recebi a incumbência de abrir este seminário que, pela excelência dos palestrantes e do público assistente, será profícuo em resultados.

Volto a dizer, certamente sou a pessoa menos categorizada para poder falar aos senhores sobre esse tema. Mas eu quero, mais uma vez, expressar os meus agradecimentos, aplaudir a iniciativa. São iniciativas assim que nos levam, com muita tranquilidade, com muita serenidade, a estudar algo que todos nós, de alguma forma, desconhecemos.

Oportuno que, neste ambiente acadêmico, institucional, de muito interesse, de muita responsabilidade e de muita humildade, consigamos, no Estado de São Paulo, dar um norte às nossas atividades sem que os reflexos da aplicação da lei nos tragam emperramentos indesejáveis.

Por fim, apresento congratulações a todos os ouvintes e, de forma especial, ao Diretor da Escola Paulista da Magistratura, aos organizadores deste evento e aos palestrantes, com votos de sucesso.



Registros Públicos



O impacto das novas tecnologias nos Registros Públicos



A questão da proteção de dados, o



ANTONIO CARLOS ALVES BRAGA JÚNIOR
Juiz Substituto em Segundo Grau do Tribunal de Justiça
do Estado de São Paulo

Corregedor falou aqui em pânico, não entramos em pânico, mas “parece” que é exatamente isso que está acontecendo no mundo: pânico! De repente, uma explosão de preocupações aí pelo mundo. A lei europeia, a lei brasileira, muito inspirada na lei europeia, e discussão em todos os cantos.

Impacta governo, impacta toda a sociedade civil, todos os tipos de serviços, empresas, atividades puramente privadas vão ser profundamente impactadas por essa lei e pelas novas regras.

O interessante é: dados sensíveis, dados que digam respeito à vida privada, estiveram aí desde sempre. Qual a novidade, então? A novidade são os meios pelos quais esses dados são captados, armazenados, tratados, eventualmente comercializados, eventualmente vazados, de maneira não intencional, ou por ataques. Não intencional por parte de quem os detém, por puras falhas de sistemas que deixam bancos de dados gigantescos abertos; intencionais, por ataques de *hackers*.

Notícias como “Facebook. Devassadas 68 milhões de contas com login e senha” são impressionantes. A novidade é essa, a apreensão se dá diante dos novos meios pelos quais a informação é tratada.

Novos meios para tratar a informação: conhecimento humano dobra em prazos cada vez menores

Para aplicarmos a lei, precisamos conhecer esses meios, conhecer essas ferramentas, saber de que estamos tratando. Quais são esses meios, quais são essas maneiras de coletar e tratar dados? Mas é impossível estabelecer isso. Isso está em permanente construção, em velocidade acelerada.

O conhecimento humano vai dobrando em prazos cada vez menores. No passado, foi a cada 500 anos, a cada 100 anos, a cada 50. Hoje já se fala de algo em torno de 13 meses. Em algum momento falaremos de 13 horas. E as ferramentas para tratar isso brotam do chão em velocidade impressionante. Não temos como mapear isso totalmente. Está acontecendo enquanto estamos discutindo.

A ideia aqui é muito mais a reflexão, pensar a respeito, por isso começo falando de um ecossistema digital. Onde

nos inserimos? Eu estou falando de todos: estados, órgãos de Estado, governo. Estou falando de iniciativa privada, estou falando do serviço extrajudicial, que permeia esses dois mundos, uma atividade privada, mas de prestação de serviço público.

Não há mais o que discutir sobre a necessidade ou conveniência do emprego das tecnologias digitais; já é uma conversa ultrapassada. O que temos de considerar é o uso de todas as ferramentas digitais como parte de um ecossistema, como parte de um meio ambiente, um *habitat*, onde estão todas as “espécies vivas”. Quem são as espécies vivas? São órgãos de governo, são cidadãos, são empresas, todos interagindo cada vez mais entrelaçados, cada vez com mais integração de dados, com interoperabilidade, serviços conectados, serviços que conversam entre si automaticamente.

Caminhamos para a era em que as máquinas conversarão diretamente entre si, sem intermediação humana, a internet das coisas. Esse é o ecossistema, é disso que estamos tratando, é isso que está acontecendo neste momento, é disso que temos que nos ocupar.

Integração do serviço extrajudicial internamente e com ambiente externo é a grande transformação em andamento

Nesse ecossistema, onde tudo caminha para a integração, como o extrajudicial se posiciona? Há tempos se discute isso. O que é usar tecnologia digital? Imagino ambientes onde naveguem todos os serviços extrajudiciais que serão vistos sem distinção pelo usuário.

O usuário não precisa saber a diferença entre registro civil de pessoa natural e registro de títulos e documentos. Ele não tem que entender essa diferença. Mas ele tem que obter o serviço de maneira fluida, independentemente de quem cuida daquela prestação específica. A integração do serviço extrajudicial, internamente e com o ambiente

externo é a grande transformação em andamento.

O extrajudicial tem como um dos aspectos essenciais da atividade dar publicidade aos atos. É uma intenção, um objetivo, uma necessidade das sociedades desde sempre, desde a Antiguidade. Alguns atos, era importante que fossem de conhecimento público.

No passado, como é que se fazia? Esses atos, que era importante fossem do conhecimento público, faziam-se na praça pública, na presença de todos. Aos poucos, com o crescimento dos agrupamentos humanos, isso passou a não bastar mais. As comunidades aumentaram de tamanho e a parcela de pessoas a presenciar o ato já não era representativa. Como é que se assegura a publicidade? Tivemos que documentar, que escrever. Na pedra, na madeira, na argila, no papiro. E aí vem toda a história que os senhores sabem muito melhor do que eu.

De repente, deparamos com essa questão... A minha atividade típica é assegurar ampla publicidade aos atos, e cai do céu essa hecatombe, que é: protejam os dados do cidadão, protejam os dados sensíveis, não permitam que os dados sejam mal utilizados.

Equilíbrio entre publicidade e privacidade

Como fazer esse equilíbrio entre publicidade e privacidade? Como é que se faz isso? Não tem resposta pronta. Não tem. Nem sabemos o tamanho do problema.

Eu comparo um pouco a assimilação da Lei de Proteção de Dados com a assimilação do Código Defesa do Consumidor. Veio a lei, tinha prazo, entrou em vigor, foi um rebuliço. Afetou governo, maneira de atender o cidadão, todo mundo.

Quanto tempo levou para realmente podermos dizer que alcançamos algum nível de maturidade? Não menos que dez anos. Dependeu de todas aquelas decisões judiciais dizerem: “Isto é legal”, “Não, isto é ilegal”, “Isto é muito grave”, “Isto não tem como evitar, faz parte de um transtorno ao qual o cidadão está sujeito”.

Essa distinção do que era infração à lei, e do que não era, foi construída passo a passo, grau a grau. É isso que eu entendo que vai acontecer. Mas em breve a lei vai entrar em vigor, e já tem consequências, tem penalidades, tem desdobramentos.

O que o extrajudicial tem pela frente? Proteger os dados do uso indevido, proteger de vazamentos. Tem que ingressar totalmente nesse ecossistema digital e, ao mesmo tempo, garantir a longevidade dos dados, garantir o acesso à história.

Para o extrajudicial, ir ao futuro é tão importante

quanto manter a ponte para o passado. Se eu perder a ligação com o passado, com o histórico dos dados, dos documentos, das informações, o serviço extrajudicial deixa de ter razão de existir.

Só uma curiosidade... Ontem eu estava na casa da minha mãe e vi, na sala, um porta-retrato, uma foto em preto e branco que eu não conhecia. Parecia quase uma gravura. Era uma foto antiga bem esmaecida. Fiquei até na dúvida: “É foto mesmo ou é gravura? Eu acho que é foto”. Aí, vi atrás: “Fazenda não sei o quê, no município de Monte Mor, foto de 1905”. Uma fazenda que foi do meu bisavô, e eu nem sabia da história. E meu avô está criança ali naquela foto.

A primeira coisa que me veio à cabeça foi: “Será que uma foto digital duraria 115 anos?”. Essa foto está lá do jeito que foi tirada. Ninguém migrou essa foto. Talvez ela tenha migrado de caixa, de gaveta, mas a foto em si é a mesma. Ela perdeu muito da sua informação, mas eu ainda reconheço ali uma casa, uma árvore, as crianças, bicicleta.

Muito discutimos quando tratamos da gestão documental no Rio de Janeiro, no Arquivo Nacional, sobre a longevidade dos dados. Como é que se vai para o mundo digital e se garante que não se vai perder o fio da meada? Muita coisa está se perdendo no mundo digital, porque a sociedade está preocupada com o hoje e com o amanhã. O ontem já não interessa mais. O ontem cada vez tem menos relevância até que a pessoa precisa do ontem, aí ela vai esbravejar. A essência da atividade extrajudicial é exatamente preservar esse ontem para sempre. É mais crítico do que para o Judiciário.

Uso de dados de redes sociais: algoritmos previram o brexit e a eleição americana

O *Cambridge Analytica* e o Facebook, esse escândalo que tomou conta das notícias... A notícia “Privacidade hackeada” mostra os bastidores do escândalo da *Cambridge Analytica* e do Facebook. “Facebook é multado em 5 bilhões de dólares nos Estados Unidos.”

Tem um documentário interessante sobre isso. O que foi a história do *Cambridge Analytica*? Essa empresa britânica ficou famosa porque previu o resultado do plebiscito do *brexit*. Ela previu o resultado contra a previsão de todos os analistas que diziam: “A Inglaterra não vai sair da Comunidade Europeia”. E eles disseram: “Vai sair. O povo vai votar pelo sim”. E acertaram.

Como eles fizeram isso? Coletando dados das pessoas nas redes sociais. Dados que o cidadão coloca volunta-

“Para o extrajudicial, ir ao futuro é tão importante quanto manter a ponte para o passado. Se eu perder a ligação com o passado, com o histórico dos dados, dos documentos, das informações, o serviço extrajudicial deixa de ter razão de existir.”

riamente lá. Não necessariamente o cidadão autorizou que isso fosse feito. Foi esse o problema. Ele não autorizou que o Facebook liberasse dados para esse fim. Mas a verdade é que se trata de um dado que a pessoa disponibiliza. É quase um mural. Eu posto uma coisa no Facebook, que tem mais de 3 bilhões de usuários no mundo, e digo: “quero preservar a minha privacidade”. Tudo bem, tem casulos, tem subsistemas de fechamento da informação. Mas a verdade é que você está postando uma foto, um texto, uma opinião numa rede planetária.

Usaram esse tipo de informação. Usaram algoritmos muito poderosos, muito eficientes. Hoje em dia, não faltam recursos para isso: memória, processamento, velocidade de transmissão e algoritmos altamente poderosos. Essas ferramentas existem, eles foram capazes de desenvolver os algoritmos e conseguiram prever o *brexit*.

Isso chamou a atenção para a eleição americana. Pensaram: “Vamos usar esses caras também”, e assim o fizeram. E lá se fez a mesma coisa: uso de dados de rede social.

Analisando dados do Facebook concluíram: “cada pessoa tem de 4 a 5 mil *data points* na rede – pontos de dados, informações sobre ela. Nem ela sabe tanto sobre si própria como nós podemos saber. Podemos estabelecer o perfil de personalidade, estabelecer uma tendência. Esse cara vota conservador, esse cara vota progressista. Esse cara é liberal, esse cara é conservador nos costumes, mas na visão econômica ele é liberal”. Quanto vale isso?

É a primeira vez na história que isso está sendo feito? Óbvio que não. Sempre foi feito. Como sempre se fizeram os planejamentos de campanha política? Eu tenho que conhecer o meu eleitorado, saber onde é que eu tenho mais potencial, onde é que eu tenho menos. Isso sempre foi feito. Só que dessa vez foi feito com uma ferramenta tão poderosa e gerou um resultado tão surpreendente que estabeleceu o pânico.

Uma Comissão no Congresso Americano chama o Mark Zuckerberg para prestar depoimento. Aplica uma multa de 5 bilhões de dólares. “Isso não pode!”. Espera aí, sempre foi feito, com dados que o cidadão distribuía.

O que a *Cambridge* fazia? “Nestes estados aqui, você já ganhou. Não perca o seu tempo nem o seu dinheiro. Nestes estados aqui, você não ganha de jeito nenhum. Não perca o seu tempo, nem o seu dinheiro. Nestes estados, a bola está dividida, é aqui onde dá para virar o jogo. Concentre todo o seu tempo, seu material de campanha, aprenda sobre essas populações, sobre esses estados, sobre a história deles e vá falar para eles, vá se dirigir a eles”. E previram: “Você vai ganhar a eleição”. Deu certo.

Veio essa hecatombe, essa indignação mundial, esse documentário, que eu vejo com uma boa reserva. Sempre aconteceu. Eles só foram muito bem-sucedidos em fazer o que sempre se tentou fazer.

O fato é que houve uma enorme transformação e não tem mais volta. Gerou esse alarme, e agora o mundo inteiro vai ter que se adequar.

Governo *versus* sociedade: no meio, o extrajudicial

Tenho traçado o seguinte desenho: vejo dois grandes blocos, governo de um lado, sociedade do outro. Governo são todos os órgãos públicos. Sociedade é cidadão, iniciativa privada, empresas, corporações, associações. No meio desses dois blocos vejo o extrajudicial, atividade privada que presta serviço público.

O extrajudicial, necessariamente, tem que dialogar com esses dois lados.

A iniciativa privada vem há mais tempo fazendo o ingresso no mundo da tecnologia. Mas o governo é um grande novato. Sempre foi o mais atrasado, não se via nada de evolução em governo, em órgão público. Órgãos do Governo Federal, órgãos da Justiça sempre foram primitivos e parecia que nunca iam sair

do atraso. A Justiça parecia ser o último lugar onde alguma coisa ia acontecer.

De repente tudo muda de posição, de repente o Estado se reposiciona. Quando falo Governo, refiro-me a órgãos de Estado. É assim que o mercado de tecnologia se refere aos poderes de Estado, incluído o Judiciário. “Governo”. Então, o governo, hoje, é um enorme comprador de tecnologia. Compramos as últimas tecnologias em larga escala, investindo muito dinheiro e estamos colhendo enormes resultados e obtendo enorme economia.

O governo aprendeu. Entendeu a importância do governo eletrônico. Do outro lado, a iniciativa privada, não precisa nem falar. Já entendeu e está criando a sociedade do futuro que a gente nem bem sabe como é que vai ser.

Uma notícia bem recente: “Governo lança portal único e reunirá cesta de 1600 serviços públicos”. Isso é só Governo Federal. O anúncio é: 400 serviços públicos colocados em meio digital até o final deste ano, e 1600, até o final de 2020. Por quê? Porque já entenderam: redução absurda de custos, viabilidade da prestação do serviço, quer dizer, eficiência na prestação de serviço e boa avaliação do cidadão. Que agente público não quer isso?

O modelo tradicional de serviço público, o modelo de balcão de atendimento, está exaurido. É só colocar uma interface digital em que o cidadão antecipa o serviço de que necessita, em que escolhe serviços em um menu, que se obtém um salto de celeridade, redução de prazos e de custos. Com o sistema tradicional está provado que é absolutamente impraticável.

O exemplo vem da Estônia

A Estônia é, hoje, o melhor local para se observar o que vai acontecer com o governo eletrônico. É o país mais digital do mundo. País pequeno, temos um mapa aqui para lembrar onde fica a Estônia. É um trio, Estônia, Letônia, Lituânia, logo abaixo da Península Escandinava. Faz divisa com a Rússia. Foram controlados, esses países todos, pela União Soviética, até o desmoronamento do bloco.

A Estônia é um país de 1,3 milhões de habitantes, ou seja, um pouquinho maior do que a cidade de Campinas (SP). Era um país atrasado, pobre, sem nada, sem estrutura nenhuma, debaixo daquelas regras rígidas da União Soviética. Quando se pergunta: Como vocês conseguiram dar esse salto?” A resposta deles é: “Por pura necessidade”.

Quantas necessidades temos e que não nos moveram ainda a dar saltos parecidos? Para eles, a necessidade foi suficiente.

e-Estônia: 90% da população interage com o governo em meio eletrônico

Eles têm lá o e-Estônia, o ID Card. Recebem em casa, pelo correio, um cartãozinho com certificado digital, com todos os seus dados, fotografia, assinatura digitalizada, dados biométricos. A tecnologia em si não é novidade para nós, mas não está implantada no Brasil.

Mais de 90%, quase a totalidade da população, interage com o governo em meio eletrônico. Todos os serviços públicos funcionam em meio eletrônico. O cidadão se *loga* no sistema, se identifica, faz tudo com esse cartão. Assim ele é reconhecido. Declaração de imposto de renda, restituição. Na verdade, declaração de renda é meramente uma confirmação de declaração pré-preenchida que o governo manda para ele. “Está tudo ok? Você confirma esses dados?” Então, o prazo de restituição de imposto foi reduzido para dois dias.

e-Residence: residência legal eletrônica na Estônia permite abrir empresa

O e-Residence é uma residência legal, uma figura de imigração.

Residência Legal Eletrônica, o que significa isso? Eu, de qualquer lugar do mundo, solicito uma residência legal eletrônica na Estônia. Não preciso morar lá. Tenho uma residência legal eletrônica na Estônia, para onde nunca fui, nem irei, mas posso usar alguns serviços digitais. Por exemplo, abrir uma empresa na Estônia. Aqui tem uns dados bastante desatualizados. É uma página do Governo da Estônia. Na época, tinha lá vinte mil residentes eletrônicos. Hoje, já passa de 30 mil, e acho que está batendo os 40 mil, de 138 países. Hoje são mais de 5 mil empresas abertas por esses residentes eletrônicos.

A ideia é: você quer abrir uma empresa para uma atividade de internet, um *e-commerce*, para a qual o problema de geografia não existe? Abra na Estônia como um cidadão eletrônico, um residente eletrônico.

Fui ver como é o passo a passo para abrir essa empresa. Se você é um cidadão, residente legal e residente efetivo no território da Estônia, o processo de abertura de empresa é mais rápido. Duas horas.

Agora, se você é de fora, um cidadão eletrônico, então vai demorar um pouco mais. De 1 a 7 dias. “Olha, você

manda todos os seus documentos, preenche um formulário no *e-business register*, na internet, manda os documentos em meio eletrônico, manda sua foto. Vamos checar algumas coisas. Dando um OK, você vai ter que vir para a Estônia, passar um tempo aqui para finalizar”.

Quanto tempo? Um dia.

Nesse um dia você vai em dois lugares: a um notário e um banco. Você tem que se autenticar perante o notário e você vai ter que abrir uma conta no banco da Estônia. Ponto final. Pode ir embora, não precisa voltar nunca mais. Paga as taxas anuais da empresa e pronto.

A ideia é: “Abra a sua empresa aqui, venha ganhar dinheiro aqui, venha gerar impostos para nós aqui. Nós criamos um ambiente de negócios de maior facilidade possível.”

e-Health: rede de saúde integra hospitais, postos de saúde e de vacinação

O e-Health é o sistema de saúde eletrônico. Todo cidadão, com aquele mesmo cartão de identificação, usa todos os serviços eletrônicos. O Ministério da Saúde tem o perfil de cada cidadão e todas as informações de saúde: as receitas médicas, os exames, agendamentos, atendimentos, tudo o que diga respeito à questão de saúde dele. Precisa da emissão de uma declaração médica para renovar a carteira de motorista? Faz a solicitação via *e-Health*.

Cada usuário pode vincular pessoas sob seus cuidados ou responsabilidades. No exemplo, uma mulher tem o filho e a mãe (Hugo e Viv) vinculados ao perfil dela. Isso significa que ela tem permissão para gerenciar questões de saúde do filho e da mãe. Comprar remédio ou fazer qualquer tipo de encaminhamento.

Essa pessoa, na farmácia, apresenta o seu cartão de identificação, dá o código de identificação do paciente – no caso, pode ser o dela, o do filho ou da mãe. O farmacêutico acessa o sistema e verifica quais são as prescrições médicas que ela tem. Não existe receita em papel. Ele vai checar as identidades digitais e fornecer os medicamentos que estão prescritos pelo médico.

Tudo isso é feito em blockchain e permite o controle de acesso pelo cidadão.

A mãe, a titular dessa conta, tem como abrir ou fechar o acesso às informações de saúde do filho para quem ela quiser. Está aberto o acesso para o marido e não está aberto para essa terceira pessoa.

Por dentro da rede saúde existe uma integração entre hospitais, postos de saúde, de vacinação etc.



Estônia: melhor local para se observar o governo eletrônico

e-Ambulance: integração total do sistema de saúde

Uma parte do vídeo explica o e-Ambulance.

Tem um acidente, uma batida, colisão. Há uma pessoa machucada. Pega o nome da pessoa, faz a solicitação de uma ambulância e passa a identificação desse fulano. Pega a carteira dele: “Olha, é o fulano de tal que precisa de atendimento”. O sistema localiza o celular que está chamando, localiza a ambulância mais próxima, direciona essa ambulância para lá, e manda o perfil completo, todo o prontuário médico, para o paramédico que está na ambulância, que está com um *tablet* na mão vendo alergias, tipo sanguíneo, toda a informação, para quando chegar lá, saber de quem se trata. É a integração total do sistema de saúde.

e-Notary: notário digital

Eles têm também o e-Notary, o notário digital. A atividade é bem análoga à nossa. Os particulares, comprador e vendedor, ao chegarem a um entendimento, submetem ao notário, que gera um documento eletrônico e submete remotamente à assinatura eletrônica dos dois interessados. Em seguida, faz o encaminhamento para registro. Tudo bem rápido.

e-Land Register: simplificação e fluidez – tudo num único portal

O e-Land Register é o registro de imóveis eletrônico. Esse canal central, é o canal de dados governamental na internet, o *backbone* do governo, é o governo eletrônico da Estônia na internet. A esse *backbone*, essa grande

tubulação de dados, se conectam todos os serviços. Aqui temos o Land Register, o Notário, o e-Business Register, ou registro de empresas e o registro civil. E vejam que interessante, um Land Cadastre. Temos um cadastro territorial, que não se confunde com registro territorial. Quanto já discutimos sobre essa separação entre registro e cadastro?

Esse é o *site* do registro de imóveis, tudo em estoniano e inglês. A descrição dos serviços, toda a documentação é *online*, em um único portal. Para qualquer serviço, você precisa de instruções? Estão todas ali. Tem as explicações, os valores, como você tem que fazer, o que você precisa apresentar. É um grande Poupa Tempo, uma simplificação com grande fluidez.

Data Embassy: uma embaixada de dados em país estrangeiro

Outra coisa que eu achei fenomenal: Data Embassy. Uma embaixada de dados. O que é isso? Em 2007, houve um ataque *hacker* na Estônia. Não destruiu, mas tirou boa parte dos serviços públicos do ar. Como é que eles se protegem?

“Proteção é um problema do dia a dia, uma tentativa de sempre estar um pouco à frente do *hacker*. Para assegurar isso, armazenamos os nossos dados fora da Estônia também. Esse é o primeiro caso de uma embaixada de dados, num país estrangeiro, por força de um tratado, de um acordo diplomático. Escolhemos Luxemburgo, primeiramente, por segurança jurídica, estabilidade num país pouco sujeito a conflitos e que tem muita abertura para esse tipo de discussão”.

Então, o que é a embaixada, na prática? É um *data-center* no território de Luxemburgo, que tem as mesmas prerrogativas de uma embaixada, tem imunidade. O controle é total da Estônia. O *datacenter* é território estoniano.

É uma figura que não se encaixa nas figuras convencionais de diplomacia. Eles explicam: “Isso é uma nova figura da diplomacia”.

Eles já têm os dados replicados em vários países. Se houver um crash total, você tem como restabelecer o sistema em tempo não muito longo, e recuperar o serviço público.

I-Voting e The End of Privacy: acesso gratuito às informações para fins de pesquisa

I-Voting, sem muita novidade, voto eletrônico pela internet.

The End of Privacy tem muito a ver com o nosso assunto aqui. É um documentário... Na verdade é o título de uma pesquisa do professor Michal Kosinski, pela Universidade de Stanford. A pergunta que eles tinham era: “Seus dados digitais revelam mais a seu respeito do que seus amigos e sua família sabem?”

Onde é que está boa parte dos dados a respeito das pessoas? Facebook. Mas, não pode. Já teve o problema com a Cambridge. Então resolveram: “Vamos fazer o seguinte: vamos pedir autorização. Quem se disporia a nos ceder, gratuitamente, acesso aos seus dados no Facebook? Cada pessoa coloca na rede meio *gigabyte* por dia. Muita informação. Então, vamos ao Facebook buscar.”

Três milhões de pessoas deram gratuitamente acesso às suas informações para fins de pesquisa!

A proposta era: “Não queremos nada pessoal. Queremos apenas os dados suficientes para traçar um perfil. Nós vamos pegar só os seus *likes*... Nenhuma postagem, nenhum texto, nenhuma palavra sua. Vamos pegar só aquilo que você curtiu”.

Eles viram que, com 10 *likes*, o algoritmo conseguia traçar um perfil psicológico equivalente ao que tem o seu colega de trabalho, o quanto o seu colega sabe a seu respeito. Com 100 *likes*, conseguia traçar um perfil de personalidade equivalente ao que uma pessoa da sua família tem a seu respeito: sua mãe, seu filho, seu tio. Com 250 *likes*, conseguia um perfil mais preciso do que a pessoa que teoricamente mais o conhece, que é o esposo ou a esposa.

Na média, cada usuário no Facebook tem, hoje, coisa de 215, 220 *likes*. Só que se você recortar os adolescentes, cada um tem cinco mil. É muito dado, e é um volume crescente. É tudo exponencial. Então imagine o que é possível saber.

Perfil de personalidade a partir de fotos

Aqui um outro experimento. São fotos, retratos femininos. O sistema de inteligência artificial separou dez fotos de dez pessoas. Sobrepos as fotos e classificou da seguinte maneira: personalidade extrovertida ou personalidade introvertida.

Você vai checar a margem de acerto, e é impressionante. Uma coisa que o sistema percebeu, e do que não tinham se dado conta ainda: nas fotos cujo mapeamento do rosto informa que a pessoa é extrovertida, frequentemente, o ângulo da foto é de cima para baixo, e dos introvertidos é de baixo para cima. Coincide. A introvertida tira o *selfie* do colo, usa mais discretamente o

telefone. O ângulo da foto passou a ser um elemento de identificação de personalidade. O sistema de inteligência artificial é que descobriu isso.

Nesse experimento, também traçam um perfil de personalidade, um *personality profile*. Pegam a foto do fulano “x” qualquer, passam por várias camadas de uma rede neural, e ela dá a pontuação nessas cinco dimensões. Desenha um polígono, e isso é a representação de um perfil de personalidade.

A ideia, com esses pontos, é demonstrar o que está acontecendo, o que está a caminho. É coisa atual.

Entity resolution analisa fragmentos de informações pessoais

O *entity resolution*¹ é relativo à gestão de dados, big data, grandes bancos de dados, e ao tratamento com inteligência artificial. Vamos imaginar no banco de dados eu tenho quatro entradas com algumas informações que parecem coincidir, outras não. Então eu tenho duas entradas, duas fichas de identificação, nome igual, e embaixo, diferente, será que diz respeito à mesma pessoa, uma redundância? Ou será que são pessoas diferentes?

O que o sistema faz? É muito mais complexo do que isso, mas só para dar uma primeira ideia. Então vamos primeiro analisar as duas fichas de cima.

O nome: “Antonio A. Braga”, bate, e o endereço, Avenida Ipiranga, 165, bate. E o número, que tem formato de CPF, é diferente, e uma outra entrada que tem formato de *e-mail* é diferente. O sistema analisa: *e-mail* diferente não quer dizer nada, porque a pessoa pode ter vários *e-mails*, pode ser a mesma pessoa. CPF diferente, provavelmente é uma pessoa diferente. Eu posso ter mais de um CPF? Não, mas eventualmente eu tenho um CPF em conjunto com a minha mulher. Pode até acontecer de haver um uso duplo. Mas, em princípio, sugere que não é a mesma pessoa.

O sistema está tentando fazer o quê? Identificar *matches* perfeitos: “Eu tenho certeza de que esse, esse e esse dado são da mesma pessoa”. Identificar *matches* prováveis: “não dá para afirmar, mas provavelmente esse dado e esse dado são da mesma pessoa”. E dados relacionados: “Não é da mesma pessoa, mas tem relação com ela”. E assim se constrói toda a rede de relações.

Então, comparando com o debaixo. O nome está di-

1 A descrição do *entity resolution* depende das imagens da apresentação para ser compreensível. Basicamente, se trata de análise computacional de fragmentos de informações pessoais em um banco de dados. Mesmo com informações incompletas é possível extrair grande quantidade de identificações a partir da constatação de a) coincidências, b) incoincidências e c) possíveis coincidências.

General data	Division I	Division II	Division III	Division IV
Property number	x	x	x	x
Land Registry department	x	x	x	x
Property name	x	x	x	x
Property type	x	x	x	x
Cadastral code	x	x		
Issued progress	x	x		
Location	x	x		
Flow	x	x		
Registered property rights	x			
Owner		x		
Sanctification			x	
Mortgages			x	x
Usage rights			x	
Prescriptive rights			x	
Preliminary notations			x	

e-Land Register: registro de imóveis eletrônico da Estônia

ferente, mas é compatível. “A”, com “Alves”, “Braga” está batendo. O nome da rua, avenida, está batendo, o telefone está batendo. O telefone batendo é uma forte indicação de ser a mesma pessoa. Como os nomes batem e os endereços também, provavelmente estou falando da mesma pessoa. E o que não bate é o *e-mail*, que não é relevante.

Na terceira análise aqui, está bem diferente. Tem “A”, “C”, que não tem no primeiro; tem “Alves”, que não tem no primeiro. O endereço não bate nada, e o telefone não bate nada, mas o *e-mail* bate. O *e-mail* não batendo, não quer dizer nada, mas o *e-mail* bater quer

dizer muito, porque não tem *e-mail* pessoal para duas pessoas diferentes.

Então aqui eu tenho um *match*, sendo que o resto das informações me sugeria que não. Só para ter uma ideia do que acontece dentro de um sistema de análise, que são essas correlações feitas continuamente, limpando o banco de dados e a cada nova informação ela entra na reanálise, e eventualmente eu vou associar “A” com “D”, que são dados completamente desaparecidos, mas porque o “A”, se confirma com o “B”, o “D” confirma com o “C” e o “B” com o “C” tem correlação confirmada. Consigo amarrar “A” com “D”.

Essa possibilidade de análise faz com que todas as entradas do meu banco de dados sejam relevantes, seja para confirmar, seja para excluir, ou para eu deixar como uma possibilidade, para ser completada depois.

Pergunto: quem tem esses mega bancos de dados e está fazendo tratamento para mil finalidades, como faz com aquela regra segundo a qual depois de exaurida a finalidade para a qual o dado pessoal foi fornecido ele deve ser apagado?

Quem vai querer apagar esse dado? Se eu apago, desmonto a minha estrutura, vou enfraquecendo essa minha informação. E para quem gerencia banco de dados, se não tiver essa possibilidade de identificar, de rotular as minhas entradas, é a mesma coisa que uma biblioteca sem índice. Para procurar um livro, tenho que ir de prateleira em prateleira, corredor por corredor. Não faz o menor sentido.

Então, será que é factível? “Apague dados do seu banco de dados”?

A proteção de dados sensíveis

Proteger os dados sensíveis é uma hipótese.

Hipoteticamente, tenho aqui um ato notarial registral. O texto é do Lorem Ipsum, texto genérico. Vamos dizer que esse conteúdo, que não importa qual seja, está associado a um CPF. E para o nosso uso aqui, exclusivamente para este fim, CPF se considera dado sensível, ou seja, um dado que tem que ser protegido e, na maioria das vezes, ocultado, desatrelado daquele documento.

O CPF sabemos que não é dado sensível, mas só para servir de exemplo.

Eu tenho que emitir uma certidão desse ato notarial. O texto ali é o mesmo, mas como é que eu faço? Eu simplesmente oculto? Sim. Simplesmente ocultar o CPF é uma forma da anonimização, de exclusão dos dados de identificação.

Mas, eventualmente, pode ser que sem aquele dado eu não consiga individualizar aquele documento; ele não me tem utilidade nenhuma. Se essa informação pode ser de qualquer um, ela não me diz nada. Eu quero saber de quem é. Mas eu não posso dizer de quem é, eu não posso dizer o CPF de quem é.

Que tal se me der o *hash* do CPF? Não estou te dando o CPF, estou dando o *hash* dele e dizendo qual é a versão do algoritmo para gerá-lo. É o SHA-256.

O gerador de *hash* é um algoritmo público, aberto na internet, livre e instantâneo. Você acessa um *site*, sei lá, o *hash generator*, escolhe a versão, por exemplo, a 256. Escreve num campo o CPF, do jeito que está. Se tirar um ponto de separação, muda tudo. Para esse CPF vai dar esse *hash* sempre. É uma certeza absoluta.

Outra certeza é que é muito fácil extrair *hash* a partir do dado, mas é impraticável descobrir a informação original a partir do *hash*. Então a informação está protegida, embora eu esteja fornecendo uma certeza absoluta sobre ela.

Aí aparece um outro documento, um documento X, que eu vou confrontar a respeito de uma mesma situação. Os dois têm o mesmo *hash* relativo ao CPF. Eu não sei qual é o CPF, mas eu tenho certeza de que é o mesmo nos dois documentos, então eu consigo correlacionar esses dois documentos.

Essa é uma das milhões de coisas que vamos ter que pensar como fazer para a tal da proteção do dado pessoal. Eu não posso simplesmente apagar tudo, esconder de tal modo que nunca mais ache, porque aí perde todo o sentido. E, uma vez que tudo esteja em meios digitais, tem a questão da engenharia reversa, quer dizer, eu dou os dados, escondo alguns, mas se eu tiver uma massa de dados e os algoritmos, já se diz que é possível recompor. Mesmo que você oculte os dados, como eles estão armazenados em outro lugar, é possível aquele trabalho que fizemos agora há pouco, com as fichas de dados pessoais, de nomes (*identity resolution*).

Com a análise de dados você vai compondo, vai construindo um desenho cada vez mais detalhado. Você não precisa me dar o dado porque eu já sei, eu consigo achar, porque esse dado está em outro lugar, ele não é absolutamente secreto.

Esse é o dilema.

Em uma sociedade totalmente conectada, que é para onde estamos indo, será possível o resguardo da privacidade?





Panorama atual do Regulamento Europeu sobre a Proteção de Dados (RGPD) e os Registros Públicos.

Desafios e perspectivas



A “proteção de dados pessoais” não é,



MADALENA TEIXEIRA
Conservadora de Registro Predial em Portugal

realmente, um tema novo, pese embora a variação terminológica e a arrumação dogmática que foi recebendo ao longo dos tempos. A novidade está, sobretudo, nos instrumentos legais que vão sendo criados ou aprimorados, no sentido de a tornar mais efetiva, tendo em conta a escala e o ritmo a que os dados pessoais circulam, num ambiente cada vez mais animado por *novas tecnologias e tecnologias brilhantes*.

Introdução

Como se sabe, a “vida em relação” sempre exigiu conhecimento sobre as pessoas e, portanto, recolha e divulgação de dados pessoais, pelo que, naturalmente, o plano de tutela jurídica não radica na proteção dos *dados pessoais* em si, enquanto bem ou objeto de uma titularidade subjetiva, blindada num direito absoluto e impermeável a qualquer função social ou à pressão de outros direitos fundamentais. O intento estará antes numa delimitação rigorosa do âmbito de recolha e utilização dos dados pessoais através de instrumentos legais sólidos e coerentes de prevenção, controlo e tutela que permitam responder, com eficácia, aos perigos e aos desafios crescentes do meio tecnológico em que esses dados circulam.

Considerando que o Regulamento Geral sobre a Proteção de Dados (RGPD)¹ é hoje o instrumento basilar em matéria de proteção de dados pessoais no contexto do espaço europeu, o nosso propósito é, pois, o de sinalizar, ainda que em traços largos, o plano de interseção desse Regulamento com a atividade registral, cujo *perfil e escopo primordial* consabidamente reclamam a recolha e a divulgação de dados pessoais.

O RGPD – características gerais

Com efeito, o RGPD passou a ser o diploma fundamental em matéria de proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre cir-

culação desses dados, aplicável no conjunto de Estados-membros da União Europeia desde 25 de maio de 2018.

Esse regulamento comunga das características fundamentais dos atos legislativos desse tipo (art. 288º do TFUE)², distinguindo-se, desde logo, por ser um ato geral, ou seja, um ato que tem por destinatários a generalidade de pessoas que se situam no seu âmbito objetivo, subjetivo, temporal e espacial de aplicação e que, por isso, ficam por ele vinculadas.

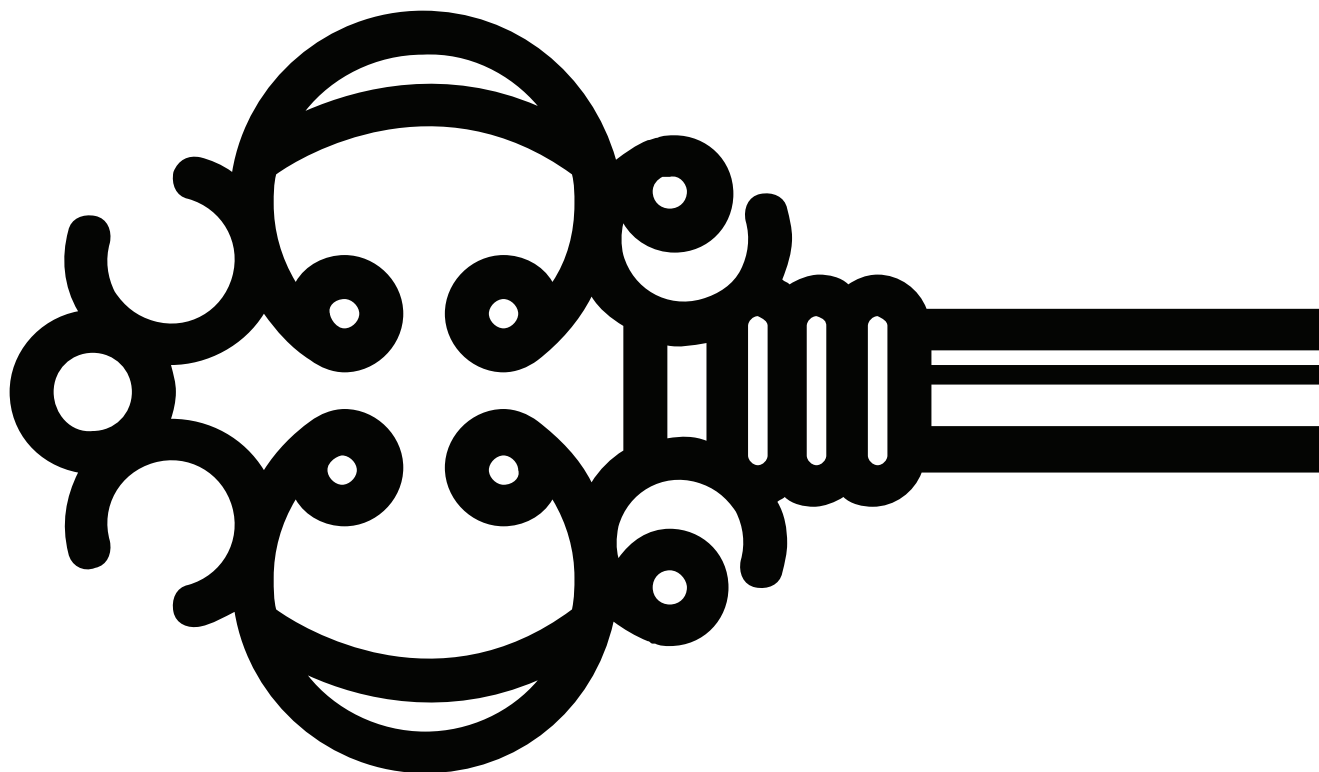
É também um ato que goza de *aplicabilidade direta*, no sentido de que se incorpora automaticamente no ordenamento jurídico de cada um dos Estados-membros sem o auxílio de qualquer mecanismo de receção, ao contrário do que acontece com as diretivas, que necessitam de um ato interno de incorporação, normalmente operado mediante um processo de *transposição*.

Mas o RGPD distingue-se, outrossim, por ser um ato obrigatório em todos os seus elementos, sem prejuízo da prerrogativa de densificação que é concedida aos Estados-Membros, designadamente nos seus Considerandos 8 e 10, e que permite a incorporação de elementos do regulamento no direito nacional, desde que para especificação ou restrição das suas regras, e não, naturalmente, para desvirtuar ou alterar o seu sentido e alcance.

Com efeito, a presunção de autossuficiência normativa atribuída aos Regulamentos não impede que, se necessário, neles se preveja ou autorize a adoção de disposições nacionais. Assim sucedeu em Portugal, com

¹ Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

² Tratado sobre o Funcionamento da União Europeia.



a aprovação da Lei nº 58/2019, de 8 de agosto, sem que tal signifique afrouxamento ao nível da obrigatoriedade ou da prevalência da matriz reguladora, que continua a ser o RGPD³.

A oportunidade do RGPD

As novas tecnologias são o bem, mas também são o perigo de vivermos nestes tempos⁴.

A racionalidade e a *occasio legis* deste regulamento, vale dizer, o seu foco e a ponderação de interesses subjacentes, aparecem espelhados no próprio regulamento, designadamente nos seus considerandos 5, 6 e 7, por referência à globalização e à internacionalização crescente das relações jurídicas e económicas, com fluxos transfronteiriços de dados cada vez mais intensos, a que se junta a marca indelével das novas tecnologias e os desafios criados pela era digital.

Constata-se, para esse efeito, o potencial de partilha,

circulação e transformação dos dados recolhidos em ambiente tecnológico, a proliferação do interesse público e privado nos dados pessoais, e a mudança de paradigma económico, social e cultural em que se constitui a sociedade da informação.

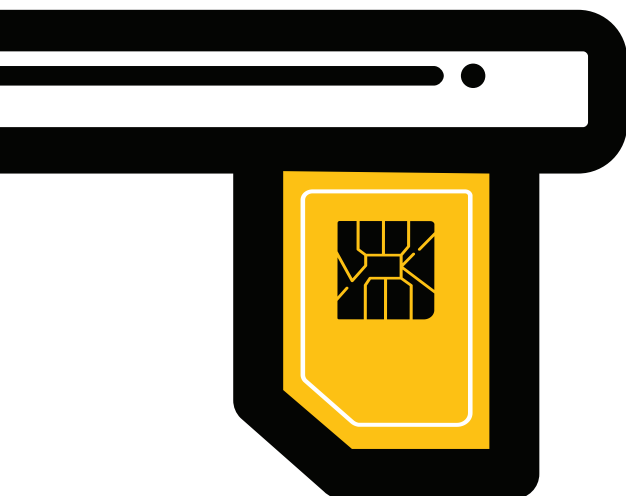
Como já vimos afirmado alhures, “na sociedade da informação não há desperdício”. Nenhuma ideia; nenhum pensamento; nenhuma reflexão se desperdiça, justamente por estar ao alcance de um clique partilhá-la com o resto do mundo, com milhões de destinatários e interlocutores. O hábito digital altera os processos de interação socioeconómica e alimenta-se da partilha dos dados pessoais para os mais variados fins.

Torna-se, por isso, evidente, a necessidade de um plano legal de proteção capaz de calibrar o desenvolvimento da economia digital segundo critérios de conformidade, e de assegurar um nível de segurança jurídica e de segurança prática que reforce a confiança das pessoas relativamente à proteção dos seus dados pessoais.

De acordo com o Considerando 4, o *tratamento dos dados pessoais deverá ser concebido para servir as pessoas*, donde o foco do RGPD não está na constrição da recolha da informação relativa à pessoa singular identificada ou identificável numa lógica de escudo contra a *sociedade da informação*, mas na criação de mecanismos de proteção da confiança e de segurança jurídica que permitam às

3 Não obstante o sumário da Lei indicar que, com ela, se assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, parece que não cabe qualquer entendimento contrário à aplicação direta e imediata do RGPD a partir de 25 de maio de 2018.

4 A expressão é inspirada em José de Faria Costa, “O Direito Penal, a Informática e a Reserva da Vida Privada”, Comunicação e Defesa do Consumidor, Coimbra, 1996, p. 308.



peçoas retirar a máxima utilidade dos canais de comunicação subsidiados pelas novas tecnologias, sem perda do controlo sobre os seus dados pessoais.

A proteção das pessoas relativamente ao tratamento de dados pessoais é um direito fundamental

Se as razões substantivas do ato legislativo em que o RGPD se traduz parecem ter sido as que se anunciam nos referidos Considerando 5, 6 e 7, o impulso foi certamente a afirmação da proteção das pessoas singulares relativamente ao tratamento dos seus dados pessoais como *direito fundamental*, assim proclamado no art. 8º/1 da Carta dos Direitos Fundamentais da União Europeia, e no art. 16º/1 do TFUE.

Tal como se nota no Considerando 1 do RGPD, esta asserção do direito das pessoas singulares relativamente ao tratamento dos seus dados pessoais como um *direito fundamental* constituiu o estímulo jurídico para reforçar a vinculatividade desse direito e prestar um contributo para a afirmação de um espaço de união económica, liberdade, segurança e justiça, tendo em vista o progresso económico e social e o bem estar das pessoas singulares.

Cabe referir que, em Portugal, o direito à proteção dos dados pessoais há muito encontrava respaldo no art.

35º da Constituição da República; norma que, no plano *infra constitucional*, foi tornada operacional com a Lei nº 10/91, de 29 de abril, a que se sucedeu, sobretudo por força da necessidade de transposição da *Diretiva 95/46/CE*, um conjunto de alterações que culminou com a Lei 67/98, de 26 de outubro.

Porém, neste momento, o RGPD é o instrumento legal que prevalece, quer por via do princípio da abertura internacional que orienta a nossa Constituição da República, quer por causa do que se usa designar por *primado do direito da União Europeia*.

Revogando a Diretiva 95/46/CE

A propósito do regulamento, uma pergunta que normalmente se faz é esta: para que um Regulamento sobre proteção de dados pessoais quando já havia uma diretiva comunitária com o mesmo objeto?

Encarando a questão numa perspectiva meramente formal, diríamos que a razão de ser de um Regulamento, em vez de uma Diretiva, radica no fato de a diretiva só vincular os Estados-Membros quanto ao resultado a alcançar, deixando, pois, às instâncias nacionais a competência quanto à forma e aos meios, e dando, assim, o ensejo a alguma variabilidade normativa no conjunto dos Estados-Membros.

Foi precisamente o que aconteceu com a Diretiva 95/46/CE, a qual foi transposta de forma fragmentada e assimétrica, criando barreiras de interpretação e da aplicação coerente e homogênea, as quais se cifraram, naturalmente, em prejuízo e enfraquecimento em termos de segurança jurídica.

Nos dizeres do Considerando 9 do RGPD, não foi, pois, a imprestabilidade dos objetivos e dos princípios contidos na Diretiva 95/46/CE a ditar a mudança legislativa; foi antes a diferenciação normativa existente em matéria de proteção de dados pessoais ao nível da União Europeia e o impacto negativo que a mesma representa em termos de segurança e de confiança jurídicas.

Do ponto de vista substantivo, a superação do esquema de proteção de dados pessoais gizado na Diretiva 95/46/CE é, sobretudo, justificada pelo volume, cada vez mais significativo, das relações transfronteiriças, o ritmo, cada vez mais acelerado, da utilização das novas tecnologias nas suas múltiplas vertentes, o caminho, sem retorno, para uma *economia digital* no conjunto do mercado interno, e a necessidade de acobertar esta nova realidade sob um manto único de proteção de dados pessoais, apto a, pelo menos, apaziguar o *sentimento*

“Uma postura de responsabilidade, de boas práticas, de transparência e de *accountability*, imposta pelo RGPD, mas adequadamente prosseguida pelos operadores econômicos, não poderá senão fomentar fidelização e vantagem competitiva no mercado.”

generalizado da opinião pública de que subsistem riscos significativos para a proteção das pessoas singulares, nomeadamente no que diz respeito às atividades por via eletrônica.

“Compliance is liberating”

Num contexto de globalização, onde o “hábito digital” está instalado e o grau de sofisticação das novas tecnologias se torna cada vez mais refinado, permitindo a circulação, fusão e transformação da informação praticamente em tempo real, é patente a necessidade de se estabelecer balizas legais mais robustas para a proteção de dados pessoais, que incutam confiança nas pessoas relativamente à utilização dos seus dados pessoais, mas, que, por outro lado, definam, com precisão, um quadro de deveres e obrigações uniforme e transversal, que elimine as distorções de concorrência e de desempenho económico potenciadas pela assimetria normativa anteriormente existente no conjunto dos Estados-Membros.

Na perspectiva dos operadores económicos, a definição de um bloco legal preciso, sólido e coerente dos deveres, obrigações e boas práticas a cargo dos responsáveis pelo tratamento de dados pessoais, e o rigor no seu cumprimento são também uma via para facilitar a própria circulação dos dados e, com isso, estimular o desenvolvimento da sociedade e da economia digital. Em vez de dificuldade, a *compliance* em matéria de tratamento de dados pessoais pode bem ser entendida como uma *oportunidade*, porquanto uma empresa que cumpre todos os deveres impostos pelo RGPD e consegue demonstrar esse cumprimento, é certamente uma empresa que está em condições de passar uma mensagem positiva e séria ao seu cliente quanto ao modo como os seus dados pessoais são utilizados. Dito de outra forma, uma postura de responsabilidade, de boas práticas, de transparência e de *accountability*, imposta pelo RGPD, mas adequadamente prosseguida pelos operadores

económicos, não poderá senão fomentar fidelização e vantagem competitiva no mercado.

O papel do RGPD num mundo (ainda) com papel

Como vivemos num tempo em que a tecnologia é a solução para tudo; “*é sempre uma resposta, mesmo que a ordem social não tenha feito nenhuma pergunta*”, compreende-se que o tratamento de dados pessoais em ambiente eletrónico seja o referente mais notório do Regulamento.

Contudo, o considerando 15 é claro no sentido de que a proteção das pessoas singulares relativamente ao tratamento dos seus dados pessoais também alastra aos ficheiros manuais, desde que estruturados de acordo com critérios específicos, seja qual for a forma ou o suporte utilizado (eletrónico ou de papel).

Logo, mesmo que o continente ou suporte seja o papel, e não um ambiente eletrónico, desde que se trate de informação pessoal centralizada e estruturada, de acordo com critérios selecionados em função do objetivo prosseguido com a recolha, e que, portanto, permita um acesso fácil, designadamente para ulterior utilização, cumpre aplicar as regras do RGPD⁵.

O RGPD – evolução ou disrupção?

Ainda assim, o pano de fundo onde o RGPD se move é claramente o da *digitalização da atividade social e económica*, e o grau de vulnerabilidade das pessoas singulares relativamente ao tratamento dos seus dados que se visa encurtar tem como foco principal os desafios, mas também as oportunidades geradas pela globalização e pela evolução tecnológica.

O plano do RGPD não é, contudo, o de se constituir em entropia ao desenvolvimento da economia digital,

5 Cfr., Acórdão do Tribunal de Justiça da União Europeia, de 10 de julho de 2018, Proc. C-25/17.

nem é, como atrás sublinhamos, o de seguir uma linha de objetivos diversa daquela que norteou a Diretiva 95/46/CE. O propósito é antes o de tornar mais robustas as condições necessárias para que esse desenvolvimento ocorra num ambiente de segurança prática e jurídica, conferindo às pessoas a possibilidade de *influenciar, de participar e de controlar o uso dos seus dados pessoais*. Pese embora a *jusfundamentalização* do direito à proteção dos dados pessoais ter exigido um compromisso normativo mais fino e incisivo em matéria de tratamento de dados pessoais, designadamente em matéria de *transparência*, de direito à *informação* e de reforço das *obrigações* dos responsáveis pelo tratamento dos dados pessoais, não deixamos de encontrar, no RGPD, o lastro substantivo da Diretiva 95/46/CE, que ficou expresso no Considerando 9 e se revela, desde logo, nas definições de dados pessoais e de tratamento, bem como nos princípios descritos no art. 5º, pelo que, nesta medida, talvez possamos dizer que o RGPD é mais desenvolvimento do que *disrupção*.

As decisões automatizadas e a definição de perfis

Não obstante o intento conciliador com as novas tecnologias e o desenvolvimento da economia digital que ressuma do RGPD, o reforço de garantias e as medidas de salvaguarda no domínio das decisões individuais tomadas *exclusivamente com base no tratamento automatizado*, nomeadamente as que imputam ao responsável pelo tratamento o dever de assegurar um meio através do qual o titular do direito possa obter intervenção humana na revisão da decisão, mesmo quando esta tenha sido precedida do consentimento do titular dos dados, acabam por acentuar uma ideia de “human in the loop” ou um sentido de que, em regra, o algoritmo deve suportar a decisão humana, mas não substituí-la.

Os riscos que os avanços tecnológicos podem acarretar para os direitos e liberdades das pessoas são também o motivo para uma regulamentação específica em matéria de definição de perfis e de decisões individuais automatizadas, adicionando-se, nesse segmento, conceitos e garantias essenciais à contenção do impacto negativo ou injustificado que esse tipo de atuação poderá produzir na vida dos titulares dos dados⁶.

Assim, de acordo com o preceituado no RGPD, a “definição de perfis”, descrita como qualquer forma de

tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para *avaliar certos aspectos pessoais* de uma pessoa singular, nomeadamente para analisar ou prever aspectos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações (art. 4º/4), bem como quaisquer decisões automatizadas ficam sujeitas aos princípios da proteção de dados, sendo-lhes aplicáveis, entre outros, os requisitos de licitude, lealdade e transparência fixados no art. 5º/1/a) e a limitação das finalidades ínsita no art. 5º/1/b)⁷.

No que concerne às decisões *exclusivamente automatizadas*, ou seja, às decisões tomadas através de meios tecnológicos e sem intervenção humana, também se concede ao titular dos dados o direito de não sujeição a tais decisões, *proibindo-as* quando delas resultem efeitos na esfera jurídica ou impacto prático semelhante na vida do titular dos dados e não interceda um dos fundamentos de licitude indicados no art. 22º/2º.

Delimitando o direito à proteção de dados pessoais

Não obstante o que vem sendo dito, bem mais importante e primordial é saber de *que falamos exatamente, quando falamos de proteção de dados pessoais*. Não havendo uma definição legal de “proteção dos dados pessoais”, a primeira tarefa que se impõe ao intérprete e aplicador do direito é, pois, a de delimitar o perfil do direito, localizando o “bem” que é objeto de proteção.

Ora, olhando apenas para a expressão “proteção de dados pessoais”, diríamos, intuitivamente, que o bem que recebe tutela jurídica são os “dados”, como se de um objeto de propriedade se tratasse, e que o estatuto do direito se restringe à atribuição de uma “posição defensiva” perante o tratamento dos dados pessoais.

Apesar da comodidade terminológica que se encontrou no uso desta designação (*proteção de dados pessoais*), o RGPD não deixa, contudo, de salientar, no título e no conteúdo, que *a proteção respeita a pessoas*; não a *dados*, e que não é só de “controlo e garantia” que se trata,

7 Cfr. as orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679 adotadas pelo Comité Europeu de Proteção de Dados, disponível em <http://bit.ly/2PYeJvM>.

8 No elenco destes fundamentos de licitude avulta o consentimento explícito do titular dos dados ou o cumprimento de uma obrigação jurídica, como é, por exemplo, a que respeita à definição de perfis para prevenção de fraudes e de branqueamento de capitais.

6 Cfr. Considerando 71.

mas é também de uma *posição ativa*, de influência, de participação e de autodeterminação informacional que o direito se compõe.

Logo, o direito de proteção dos dados pessoais poderá analisar-se num complexo de posições jurídicas e numa dupla dimensão, de *garantia*, mas também de *liberdade*, que toma como ponto de partida a transparência e a informação e que encontra na *licitude* e na *finalidade* do tratamento dos dados pessoais os seus alicerces estruturais.

Quem se “protege”?

Como já dissemos, o RGPD visa proteger as pessoas singulares relativamente ao tratamento de dados pessoais, deixando, por isso, de fora do seu âmbito as pessoas coletivas, designadamente as empresas e os seus sinais distintivos, como são a firma ou denominação e os contatos.

Relativamente às pessoas falecidas, diz-se, no Considerando 27, que o Regulamento não se aplica aos seus dados pessoais, mas deixa-se ao critério dos Estados-Membros o estabelecimento de regras para o tratamento desses dados. É com base nessa passagem do RGPD que se compreende a regulamentação ínsita no art. 17º da Lei nº 58/2019, estendendo a proteção a certos dados pessoais de pessoas falecidas, nomeadamente aos dados “sensíveis” ou aos que se reportem à intimidade da vida privada ou à imagem, com as ressalvas que valem para o tratamento da mesma categoria de dados pessoais de pessoas vivas (cfr. Art. 9º/2 do RGPD).

O estatuto da proteção de dados pessoais

Mas, como se protege? Que linhas de orientação e que ferramentas são então necessárias para tornar esse direito efetivo? Quais são os princípios que enformam e iluminam o sistema gizado no RGPD? Que instrumentos fundamentais acomodam o estatuto do direito à proteção dos dados pessoais?

Ora, para além de um elenco de definições ou conceitos, encontramos, desde logo, no RGPD, um corpo unitário e logicamente coerente de princípios e de regras, onde avultam a *limitação das finalidades*, a *minimização dos dados* e a *proporcionalidade*, bem como um conjunto de instrumentos operativos destinados a fazer valer as obrigações de cada um dos atores envolvidos e a verificar e monitorizar a aplicação das medidas de proteção e de organização necessárias ao seu cabal cumprimento.

Tal como na Diretiva 95/46/CE, o *core* normativo continua a assentar na *licitude* e na *lealdade* do trata-

mento dos dados pessoais como pressupostos essenciais, na *finalidade* como critério e como limite, e na *proporcionalidade*, vale dizer, na adequação, pertinência e necessidade do tratamento à luz da razão determinante da recolha, como indicadores de legitimidade para o tratamento (art. 5º).

Do mesmo passo, outorga-se ao titular dos dados pessoais um *direito de controlo*, que alastra ao tratamento com base em fundamento jurídico diverso do consentimento, e uma *liberdade de facere* que, designadamente, lhe permite consentir ou dissentir da recolha de dados pessoais e, até mesmo quando a licitude do tratamento não dependa do seu consentimento, participar e influenciar nas operações de tratamento.

Da licitude do tratamento

Diante do disposto no art. 6º do RGPD relativo à licitude do tratamento, notamos que o *consentimento* continua a figurar como fonte principal de legitimidade do tratamento de dados pessoais, exigindo-se que se trate de um consentimento informado e esclarecido quanto ao seu sentido e alcance, manifestado em ato positivo inequívoco e explícito, *maxime* quando esteja em causa o tratamento de dados pessoais sensíveis, e indexado a uma ou mais finalidades específicas (art. 6º/1/a)º.

Por outro lado, as demais disposições do aludido art. 6º, bem como outras passagens do Regulamento⁹, dizem-nos claramente que o consentimento não pode ser “sacralizado”, desde logo porque o direito à proteção dos dados pessoais não é um direito absoluto; porque o direito à proteção dos dados pessoais também carrega uma *marca social*; e porque existem outros direitos fundamentais que, com ele, pedem harmonização prática ou justo balanceamento, segundo critérios de proporcionalidade.

Daí a admissibilidade de fundamentos de licitude distintos do consentimento e alheados do exercício de vontade do titular dos dados, nomeadamente os que permitem o tratamento quando se verifique a necessidade de cumprimento de uma *obrigação jurídica* a que o responsável pelo tratamento esteja sujeito ou quando o tratamento se mostre necessário ao exercício de funções de *interesse público*, como são as funções atinentes à publicidade registral.

9 Ainda assim, não deixa de permanecer algum do “carácter ilusório” que, não raras vezes, se usou atribuir ao consentimento, sobretudo quando desse consentimento dependa o acesso a bens e serviços aos quais o titular não esteja em condições de renunciar.

10 Cfr., a título de exemplo, os Considerandos 40 a 47.

Ponto é, em qualquer caso, que o fundamento jurídico para o tratamento encontre cobertura no direito da União ou no direito de um Estado-Membro, ainda que não se exija uma lei específica para cada tratamento de dados e, como tal, possa valer uma lei para diversas operações de tratamento baseadas numa obrigação jurídica à qual o responsável pelo tratamento esteja sujeito ou inseridas no exercício de funções de interesse público (Considerando 45).

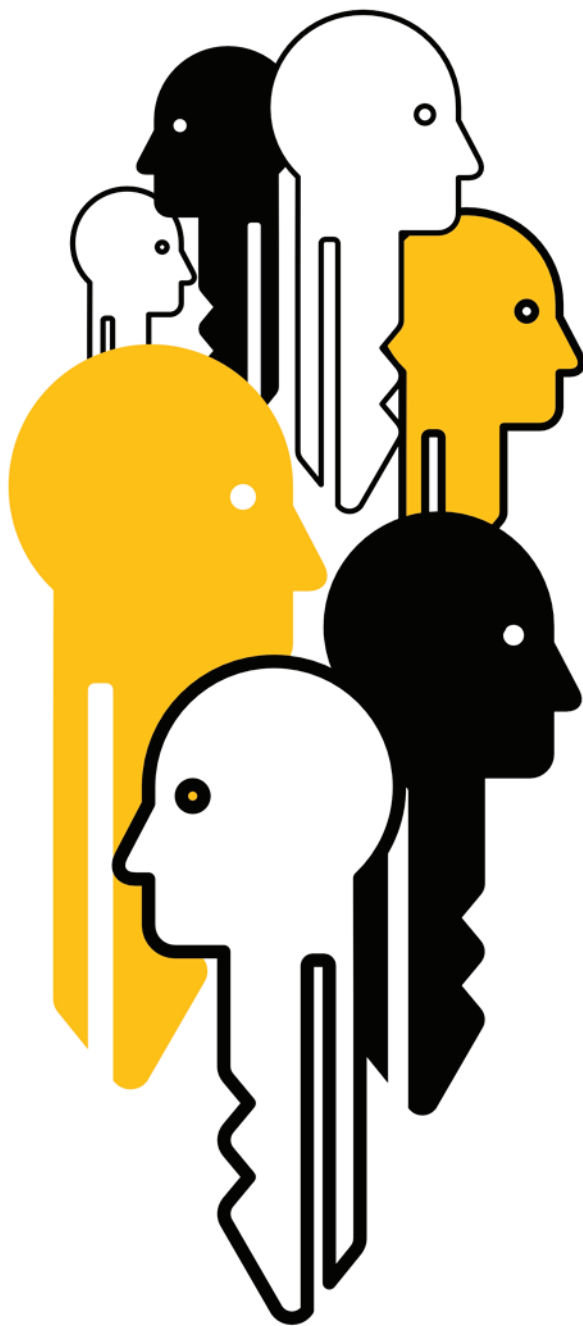
Em face do disposto no aludido Considerando 45 e no art. 6º/3 do RGPD, parece, pois, que o tratamento dos dados pessoais alicerçado no cumprimento de uma obrigação jurídica ou no interesse público no tratamento dos dados pessoais carece sempre de uma norma habilitadora e de uma finalidade cognoscível, sendo que também a *reutilização dos dados* ou a *transmissão de dados entre entidades públicas* para finalidades distintas das que determinaram a recolha se encontram balizadas por critérios específicos, nos quais não cabe, naturalmente, uma autorização legal de desvio de finalidade do tratamento que constitua uma permissão genérica e permanente, ancorada numa proclamação abstrata de interesse público.

O interesse legítimo do responsável pelo tratamento ou de terceiros

Outro dos fundamentos de licitude do tratamento de dados pessoais admitidos pelo art. 6º é o que se descreve na sua al. f) como *tratamento necessário para efeitos dos interesses legítimos* prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança.

Tratando-se de uma fórmula legal com alguma latitude semântica, o desafio mais exigente para o intérprete é, talvez, o de deslindar o que significa “interesse legítimo”, ou qual o elemento que qualifica esse interesse como legítimo, na certeza de que, como foi sublinhado pelo órgão consultivo europeu independente em matéria de proteção de dados e de privacidade, a propósito de disposição paralela da Diretiva 95/46/CE, tal interesse constitui o *requisito inicial* para a utilização desse fundamento de licitude.

Na esteira do entendimento firmado pelo referido órgão, o interesse será legítimo se for um interesse lícito (ou seja, um interesse que respeite o direito da UE e o direito nacional aplicáveis); se for específico (vale dizer,



se estiver definido de forma suficientemente clara para permitir a realização do teste da ponderação em relação aos interesses e aos direitos fundamentais da pessoa em causa); e se representar um interesse real e atual, que não especulativo¹¹.

Com efeito, o que primeiro ressalta no literal da norma é precisamente o equilíbrio entre os diversos direitos e interesses em jogo, que se presume existir quanto aos demais fundamentos de licitude previstos no elenco do art. 6º, mas que, relativamente a esse fundamento, carece de ser assegurado pelo responsável pelo tratamento, mediante um teste específico de balanceamento, que, assim, se junta ao *teste de necessidade* que vale para quaisquer fontes de legitimidade diversas do consentimento.

Em todo o caso, importa notar que esse fundamento não poderá ser mobilizado no âmbito dos tratamentos de dados pessoais efetuados por autoridades públicas na *prosecução das suas atribuições*, posto que para este efeito se exige uma norma legal habilitadora (Considerando 47).

A finalidade e a necessidade do tratamento

Seja qual for o fundamento jurídico ou a fonte legítima, é nos princípios da finalidade e da necessidade que se inscrevem o limiar e o limite do tratamento dos dados pessoais, pelo que é com base nesses princípios, de *conhecimento ou cognoscibilidade dos fins* determinantes da recolha e de *economia de dados*, que se há de medir o seu grau de licitude.

A conhecida proposição de que “a finalidade da recolha dos dados decide acerca do seu destino futuro” não parece, assim, arredada do RGPD, porquanto se continua a estipular, no art. 5º, que os dados só podem ser recolhidos para finalidades determinadas, explícitas e legítimas, e que a recolha apenas deverá incidir sobre dados adequados, pertinentes e limitados ao necessário para a *prosecução daquelas finalidades*.

Por outro lado, embora não se repudie o desvio de finalidades ou o tratamento dos dados para finalidades diferentes das que determinaram a recolha, acrescentam-se exigências de *compatibilidade* entre a finalidade inicial e as finalidades posteriores, a concretizar em teste a realizar pelo responsável pelo tratamento, segundo os parâmetros definidos no art. 6º/4, onde deve avultar uma ponderação fina de existência de uma ligação entre a finalidade inicial e a finalidade posterior e das conse-

quências que o tratamento posterior poderá representar para os titulares dos dados.

Falhando essa compatibilidade, o tratamento posterior só se mostrará viável com o consentimento do titular dos dados ou por via de um lastro normativo que constitua uma medida necessária e proporcionada numa sociedade democrática para salvaguarda de importantes objetivos de interesse público geral (Considerando 50 e art. 23º do RGPD), refletindo-se, pois, nesse espartilho ao desvio da finalidade, um compromisso do RGPD com o princípio da finalidade e o mesmo propósito de proteção dos sujeitos contra o impacto de uma utilização abusiva ou imprópria dos seus dados pessoais que já se eliciava da Diretiva 95/46/CE.

Privacy by design e privacy by default¹²

Em face do que antecede, não é, pois, no plano dos princípios que o RGPD se afigura disruptivo. É antes no paradigma de *conformidade* e de *accountability* que se inaugura no art. 24º e se reflete com particular destaque nos conceitos de *privacy by design* e de *privacy by default* que se refere o art. 25º.

Visa-se aqui o cumprimento do *princípio de responsabilidade* que aflorava na Diretiva 95/46/CE, mas que não se lograra tornar efetivo nos termos pretendidos, suscitando-se a observância das regras atinentes à proteção de dados pessoais desde a raiz, isto é, desde o momento da concepção ou definição dos meios de tratamento, até ao momento da concretização das operações de tratamento projetadas, e exigindo-se, para o efeito, a adoção das medidas técnicas e organizativas necessárias ao cumprimento efetivo dos princípios da proteção de dados, designadamente dos princípios da finalidade e da minimização dos dados.

Do bloco de instrumentos de *conformidade* gizado pelo RGPD fazem igualmente parte exigências de documentação e de registro de atividades de tratamento, deveres ao nível da confidencialidade, da integridade e da segurança da informação, e obrigações de garantia do *direito à informação* e do *direito à explicação* que convocam os responsáveis pelo tratamento e os subcontratantes para processos de governação transparentes e plenamente orientados para o cumprimento das regras de proteção de dados e para a comprovação ou demons-

11 Cfr. Parecer 06/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento dos dados na aceção do artigo 7º da Diretiva 95/46/CE, disponível em <http://bit.ly/2M9ljgi>.

12 Não obstante a distinção a fazer entre proteção de dados pessoais e *privacy* (quer no modelo norte-americano, quer nos moldes europeus), o “poder expansivo e semântico” da palavra (*privacy*) e a “sua capacidade de atração” acabam por contaminar a terminologia e por consolidar o léxico, sendo prova disso o uso generalizado das designações “privacy by design” e “privacy by default”.

tração desse cumprimento no plano interno e externo.

Em face dos objetivos do RGPD e do “bem tutelado”, bem se compreende que o nível de exigência e de responsabilidade fixado aos responsáveis pelo tratamento de dados pessoais seja acompanhado de um bloco de sanções aplicáveis em caso de violação das regras legais definidas¹³, mas também da obrigatoriedade de designação de um encarregado da proteção de dados (*data protection officer*), que, obviamente, não se substitui ao responsável pelo tratamento dos dados pessoais na titularidade dos deveres e obrigações, mas que acaba por exercer um papel de enorme relevo no sistema de governação de dados, sobretudo no que concerne ao controlo da conformidade com o Regulamento.

Refrações na atividade registral

Feita esta descrição do panorama geral do regime jurídico da proteção de dados pessoais, é agora tempo de apurar de que modo é que as disposições nele contidas se refletem na atividade registral e se harmonizam com o princípio da publicidade formal subjacente aos registros públicos.

Tendo em conta a definição posta no RGPD, sabemos que por dados pessoais se entende a informação relativa a uma pessoa singular (titular dos dados) identificada ou identificável, valendo os sinais físicos, fisiológicos, genéticos e mentais da pessoa, mas também os elementos de ordem econômica, cultural ou social que servem de referência para a sua identificação.

Vistas as coisas à luz da informação registral, é verdade que não são só os dados de identificação dos sujeitos dos fatos jurídicos que contam como dados pessoais e que também podem contar o número da matrícula do imóvel ou da entidade mercantil, posto que se trata de elementos que permitem identificar os titulares dos direitos inscritos ou as pessoas que figuram como sócios, gerentes ou administradores das sociedades comerciais. Porém, os dados pessoais recolhidos, por si só e desligados dos fatos jurídicos que os transportam, pouco ou nada revelam sobre as relações jurídicas do seu titular ou sobre as vicissitudes pessoais ou patrimoniais produzidas na sua esfera jurídica.

Daí que quando se fala de dados pessoais, no sentido de informação pessoal, não caiba uma correlação na-

tural com o *direito à privacidade*, quer este direito seja entendido numa acepção mais restrita de “*espaço de reserva irredutível das manifestações que a pessoa quer, e a comunidade acha legítimo que se queira, que permaneçam ocultas*”, quer se procure uma noção mais aberta “*de direito ao controlo da informação sobre a vida privada, por oposição à vida pública ou social da pessoa*”¹⁴.

Como alguma doutrina se encarrega de salientar, a *privacidade* e o *direito à reserva da vida privada* não ocupam o espaço próprio do *direito à proteção de dados pessoais*, porquanto esta se encontra associada à *informação existente e conservada sobre o indivíduo e não ao seu desenvolvimento existencial, aos seus comportamentos adotados enquanto tais ou socialmente projetados*, e, deste modo, respeita a qualquer tipo de informação pessoal, independentemente da sua natureza privada¹⁵.

Queremos, com isto, sublinhar que o *direito à proteção de dados pessoais* (ou *direito à informação pessoal*) não se confunde com o *direito à privacidade* e que os mecanismos que importa implementar para garantia daquele direito não são intercambiais nem substituem aqueles que o Direito Registral vai encontrando para resguardar fatos jurídicos que se encontram recobertos pela intimidade da vida privada, como são, por exemplo, a adoção plena ou a mudança de sexo.

Como já tivemos oportunidade de sublinhar noutra sede, a informação recolhida no âmbito da atividade registral (civil e predial) é, por definição, uma *informação comunicável*, posto que se destina essencialmente a tornar cognoscível por *terceiros* certos fatos jurídicos que estes à partida desconhecem, por neles não terem participado, e permitir que, com base no conhecimento

14 Por não existir entre nós um direito à privacidade como o que é reconhecido no direito norte-americano, tona-se difícil delimitar um conceito de privacidade. Por ser um conceito tão elástico e obscuro receia-se a sua pouca prestabilidade para o discurso jurídico. Ainda assim, analisando a privacidade pelo lado do interesse que o direito visa proteger, entende alguma doutrina que a ideia geral que subjaz à tutela jurídica da privacidade é a de permitir ao titular evitar ou controlar a tomada de conhecimento ou a revelação de informação pessoal, ou seja, *daqueles fatos, comunicações ou opiniões que se relacionam com o indivíduo e que é razoável esperar que ele encare como íntimos ou pelo menos como confidenciais e que por isso queira excluir ou pelo menos restringir a sua circulação* (Cfr. Paulo da Mota Pinto, “O Direito à Reserva sobre a Intimidade da Vida Privada”, Boletim da Faculdade de Direito de Coimbra, vol. LXIX, Coimbra, 1993, p. 508).

O mesmo Autor nota, ainda assim, que a vida privada não se distingue da vida pública segundo um critério puramente espacial, dependente do local onde os fatos ocorreram, pois certos acontecimentos ocorridos em público podem igualmente ser protegidos pela reserva da vida privada. Segundo o Autor, deve valer como orientação geral que *vida pública* será a vida social, mundana, da pessoa, que, portanto, diz respeito ao público, e que *vida privada* é a que o titular não quer partilhar com os outros e que a ele unicamente respeita (Cfr. “A Proteção da Vida Privada e a Constituição”, Boletim da Faculdade de Direito de Coimbra, vol. LXXVI, Coimbra, 2000, pp.164/165).

13 Na legislação interna portuguesa, para além das contraordenações puníveis mediante sanção pecuniária, foram configuradas como crime, punível com pena de prisão, as condutas mais graves, por exemplo, a utilização de dados de forma incompatível com a finalidade da recolha (cfr. arts. 46º e ss. da Lei nº 58/2019).

15 Cfr. Alexandre de Sousa Pinheiro, *Privacy e proteção de dados pessoais: a construção dogmática do direito à identidade informacional*, AAFL, 2015, pp. 771 e ss.

“Ponto é não perder de vista a finalidade do registro, porquanto é nessa finalidade que radica a licitude e o limite para o tratamento dos dados pessoais. Ponto é não esquecer que os dados são das pessoas e não daqueles que os recolhem ou conservam.”

desses fatos, se possa extrair uma conclusão acerca da situação jurídica da pessoa singular ou do prédio¹⁶.

Porém, não faltam exemplos de cautelas legislativas destinadas a restringir o *princípio de publicidade formal absoluta* que vigora entre nós e que é tributário de um princípio constitucional de “administração aberta e transparente”, como são as que se relacionam com a adoção plena, a mudança de sexo ou a perfilhação, ou aquelas que se destinam a apagar o estigma da insolvência provocado pelo registro civil dos fatos jurídicos correspondentes.

Registrar significa sempre tratar dados pessoais

Seja como for, quer a informação pessoal se integre em atos recobertos pela *reserva da intimidade da vida privada*, quer se trate de dados pessoais contidos em atos que se desenvolvem num *plano da vida em relação*, que, pela sua natureza e eficácia *erga omnes*, reclamam publicidade ou conhecimento público e, por isso, ficam de fora “do espaço de reserva irredutível das manifestações que a pessoa quer, e a comunidade acha legítimo que se queira, que permaneçam ocultas”¹⁷, existirá sempre tratamento de dados pessoais, na acepção contida no art. 4º/2 do RGPD.

Por outro lado, haverá sempre sujeição ao plano normativo contido no RGPD, independentemente do grau de maturidade tecnológica associada a cada sistema de registro e mesmo que a informação registral continue, total ou parcialmente, incorporada e estruturada em ficheiros manuais ou em suporte de papel.

Consabidamente, os sistemas de registro público são

antes de mais sistemas de informação, dado que a sua função essencial radica precisamente na recolha e organização de um conjunto de dados pertinentes à situação jurídica das pessoas singulares (registro civil) ou dos prédios (registro predial), e na sua publicitação a terceiros.

Lograr esse desiderato, implica, naturalmente, proceder à recolha, registro, organização, estruturação, conservação e divulgação de dados pessoais, na definição dada pelo art. 4º/1 do RGPD, por meios automatizados ou não automatizados, em ambiente eletrónico ou em ficheiros manuais.

Como se protegem as pessoas relativamente ao tratamento dos seus dados pessoais no âmbito da atividade registral?

Sabendo-se que registrar significa sempre tratar dados pessoais e que o direito à proteção dos dados pessoais é um direito fundamental, que não se confunde com o direito à privacidade, a questão que aqui se coloca é a de saber como se protegem as pessoas relativamente ao tratamento dos seus dados pessoais no âmbito da atividade registral.

Tendo em conta o *estatuto* do direito à proteção de dados pessoais desenhado no RGPD, não temos dúvidas em afirmar **a)** que também o tratamento dos dados realizado pelos Registos Públicos pedirá um fundamento jurídico ou uma fonte legitimadora; **b)** que também a recolha e o destino dos dados neste domínio se encontram balizados pelos *princípios da finalidade e da necessidade*; **c)** e que também aqui se impõe cumprir, e fazer cumprir, todas as exigências em matéria de *segurança e integridade da informação*.

Mas estarão os registros públicos preparados para aplicar o RGPD e passar o filtro dos princípios e das exigências que moldam o paradigma de proteção insito nesse instrumento legal?

a) O critério de licitude

Diz-se, no Considerando 4 do RGPD, que o tratamento de dados pessoais deverá ser concebido para *servir as*

¹⁶ “A informação contida no registo predial eletrónico: os dados pessoais. Recolha, uso e limitações à luz da privacidade no ordenamento jurídico português”, Revista de Direito Imobiliário (RDI) nº 81, jul./dez. 2016, São Paulo.

¹⁷ José de Faria Costa, “O Direito Penal, a Informática e a Reserva da Vida Privada”, cit., oferece a escritura pública de compra e venda de um imóvel como exemplo de um ato que se desencadeia no círculo comunicacional da vida privada, mas que, porém, nada tem de íntimo e antes se encontra vocacionado para a dimensão externa do nosso modo de ser.

peessoas, e, na verdade, não custa ver na recolha, organização e divulgação da informação feita pelo registro civil um tratamento de dados pessoais que pode servir o titular desses dados, na medida em que também concorre para o afirmar juridicamente como indivíduo e o distinguir publicamente das demais.

Da mesma forma, o tratamento de dados pessoais no registro predial poderá servir os titulares desses dados, designadamente quando o distinga como titular de um direito sobre o prédio, permitindo consolidar a oponibilidade do seu direito em face de terceiros e beneficiar da cognoscibilidade geral provocada pela publicidade registral e das suas consequências jurídicas.

Não é, porém, nessa ilação de benefício que se encontra um critério de legitimidade para as operações de tratamento de dados pessoais realizadas pelos serviços de registro. As condições de licitude do tratamento dos dados pessoais estão estipuladas no RGPD e é nesse elenco que devemos procurar o fundamento de licitude aplicável (art. 6º).

Compulsado tal elenco, torna-se, para nós, clara a possibilidade de subsunção da atividade registral nas hipóteses previstas nas als. **c)** e **e)** (*cumprimento de obrigação jurídica e exercício de funções de interesse público*), pelo que é nesse segmento do RGPD e nas disposições legais que suportam a publicidade registral e que, para o efeito, demandam que se proceda à recolha, organização, conservação, atualização e divulgação de informação pessoal pertinente ao escopo e à função de cada um dos setores de registro, que localizamos a fonte legitimadora para o tratamento de dados pessoais (cfr. art. 6º/3).

Como já vimos, o fato de o direito à proteção de dados pessoais ser um direito fundamental não o transmuta em *direito absoluto*, nem lhe retira uma função social, e por isso se aceita que o tratamento de dados pessoais necessário ao exercício de funções de interesse público ou ao cumprimento da obrigatoriedade do registro não deva ficar dependente da vontade (consentimento) do titular dos dados e que deva intercorrer uma harmonização ou justo balanceamento com outros direitos e interesses, neste caso, com o *direito à informação* e o escopo de segurança jurídica que preside aos sistemas de registro.

b) Finalidade

Importa, contudo, notar que, seja qual for a fonte legitimadora, a finalidade é sempre o ponto de partida e o ponto de chegada para o tratamento dos dados pessoais, pelo que, também nesse contexto, se exige uma razão precisa, explícita e legítima que justifique a recolha e

que, ao mesmo tempo, delimite os responsáveis pelo tratamento. Não é, assim, admissível qualquer “norma em branco” que permita o tratamento dos dados pessoais para qualquer finalidade, para uma “utilização pública ou privada da informação pessoal recolhida independentemente da finalidade” ou para um tratamento posterior com desvio de finalidade, como se os dados recolhidos deixassem de pertencer às pessoas para passar a pertencer aos responsáveis pelo seu tratamento.

Considerando que o registro civil tem, historicamente, por função publicitar as vicissitudes atinentes à condição jurídica das pessoas singulares, tendo em vista fixar autenticamente a sua individualidade jurídica e servir de base aos seus direitos civis, e que o registro predial tem por finalidade publicitar a situação jurídica dos prédios tendo em vista a segurança do comércio jurídico imobiliário, é bom de ver que o tratamento de dados pessoais no âmbito da atividade registral há de ter por limiar o escopo de cada um desses sistemas de registro.

Pela mesma ordem de razão, o desvio de finalidade, isto é, a reutilização dos dados pessoais para finalidades distintas das que determinaram a recolha só logrará licitude, à luz do RGPD, se resistir ao teste de compatibilidade; se puder contar com o consentimento do titular dos dados; ou se estiver alicerçada numa medida necessária e proporcionada numa sociedade democrática para salvaguarda de importantes objetivos de interesse público geral.

Fora dessas condições, a divulgação, transmissão ou utilização dos dados torna-se abusiva, dando lugar ao quadro sancionatório legalmente previsto, onde também se pode incluir como sujeito passivo o responsável pelo tratamento e, portanto, aquele que se encontrasse obrigado à conservação dos dados pessoais.

Minimização e proporcionalidade

A finalidade constitui, assim, um pressuposto de licitude do tratamento de dados pessoais, mas também o parâmetro para a *economia de dados* imposta pelo RGPD, demandando que o tratamento se limite aos elementos adequados, pertinentes e necessários à finalidade determinante da recolha (princípios da proporcionalidade e da minimização dos dados).

Visando à mesma ideia nuclear de ponderação ou concordância prática dos interesses colidentes em presença, concede-se ao titular, no art. 17º do RGPD, um direito a obter do responsável pelo tratamento o apagamento dos seus dados pessoais, *maxime* quando estes deixem

de ser necessários para a finalidade que motivou a sua recolha ou tratamento, pelo que uma questão que assume particular pertinência é a de saber se, relativamente à informação registral, também cabe o exercício desse direito ao apagamento dos dados ou, pelo menos, uma reserva de acesso e de divulgação, nomeadamente quando os fatos jurídicos que transportaram a informação pessoal em causa já se extinguíram.

Ora, se consideramos que a informação registral constitui, em qualquer caso, um *arquivo histórico* dos fatos que integraram a situação jurídica das pessoas singulares (registro civil), dos prédios (registro imobiliário) e das entidades mercantis (registro comercial), que, a todo o tempo, poderá ser mobilizado para realização e prova das finalidades que o determinaram, dificilmente se logrará preencher as condições fixadas no RGPD para o exercício do direito ao *apagamento dos dados*.

Parece-nos ter sido esse o entendimento seguido pelo Tribunal de Justiça da União Europeia (TJUE), no processo C-398/15 (S. Manni), ao decidir, na vigência da Diretiva 95/46/CE e a propósito de informação pessoal constante de registro comercial, que os Estados-Membros não podem garantir às pessoas singulares o direito de obter, após um determinado prazo a contar da dissolução da sociedade, a supressão dos dados pessoais que lhes dizem respeito.

Ainda assim, não deixou de se admitir, no mesmo Acórdão, a possibilidade de alguma reserva no acesso à informação e, desse modo, alguma restrição ao princípio de publicidade formal absoluta, em situações especiais e com base em razões preponderantes e legítimas relacionadas com o caso concreto, desde que tal limitação de acesso aos dados pessoais seja consentida pela ordem jurídica do Estado-Membro¹⁸.

c) Conformidade

Prosseguindo o teste de articulação do direito à proteção de dados pessoais com o princípio da publicidade formal que sustenta os sistemas de registro, não menos importante do que atentar aos princípios da licitude, da finalidade, da qualidade dos dados e da proporcionalidade, é acautelar, no âmbito da atividade registral, o exato cumprimento das regras de conformidade e de responsabilidade fixadas no RGPD, incorporando os conceitos-chave da proteção de dados pessoais e os deveres de transparência e de informação nas dinâmi-

cas procedimentais, e adotando as medidas técnicas e organizativas adequadas à proteção dos dados pessoais “*desde a conceção e por defeito*”.

Tal desiderato pedirá um investimento tecnológico capaz de blindar a informação registral contra brechas de segurança, acessos indevidos e utilizações abusivas (*integralidade e confidencialidade*) e envolve requisitos mínimos de rede e de sistemas de informação, que obviamente ganham se forem uniformes e desenhados de forma transversal a todos os serviços de registro da mesma espécie¹⁹.

Todavia, para que o modelo de proteção de dados desde a *concepção* e por *defeito* consagrado no RGPD possa ser implementado com eficácia, importará, certamente, assegurar aquilo que já ouvimos designar por “privacy by education”, e que passa, dentro de cada serviço de registro, por uma ação permanente de sensibilização, formação e consciencialização acerca do sentido e alcance do direito à proteção de dados pessoais e do seu regime jurídico.

Na mesma linha de pensamento, a essa cultura de conformidade e marca de transparência a cargo dos responsáveis pelo tratamento dos dados, há de somar-se, por parte dos titulares dos dados, um conhecimento mais fino das prerrogativas que o RGPD lhes concede e a compreensão do seu direito à proteção de dados pessoais não apenas como garantia, mas também como liberdade, ou seja, como *autodeterminação informacional*.

Conclusão

Feito este pequeno sumário de implicações do RGPD nos sistemas de registro, não encerramos com a convicção de termos superado todas as dúvidas, contudo, resta-nos o tempo da aplicação prática e os subsídios doutrinários que se forem produzindo para eliminar as dificuldades de ajustamento ou de articulação entre o direito à proteção de dados pessoais e o direito à informação registral.

Entretanto, para o ordenamento jurídico sobra a necessidade de densificação do regime da proteção de dados pessoais na legislação privativa dos registros, de modo a garantir uma justa ponderação e uma harmonização mais fina entre esse direito e o *princípio da publicidade formal* em vigor nos sistemas de registro, sobrando, para cada um de nós, o dever de compreensão do espaço

¹⁸ Acórdão disponível em <http://bit.ly/2Qx7Q4z>.

Cfr. ainda Comunicado de Imprensa nº 27/17 do TJUE, disponível em <http://bit.ly/37iNuTd>.

¹⁹ Em Portugal, optou-se por definir, na Resolução do Conselho de Ministros nº 41/2018 (disponível em <http://bit.ly/2MDduRj>), os requisitos técnicos mínimos das redes e sistemas de informação exigidos ou recomendados a todos os serviços e entidades da Administração Pública.

próprio do direito à proteção de dados pessoais, mas também, certamente, o *dever de informar*, porque é essa a vocação dos registros públicos.

Ponto é não perder de vista a *finalidade do registro*, porquanto é nessa finalidade que radica a licitude e o limite para o tratamento dos dados pessoais. Ponto é não esquecer que os *dados são das pessoas* e não daqueles que os recolhem ou conservam.





**A proteção
registral de
dados pessoais
e sistemas
registrais
europeus.**

**Medidas práticas
– a experiência
portuguesa e
europeia**



Em linhas gerais, grande parte do que



SOLANO DE CAMARGO

Doutor e Mestre em Direito Internacional pela Faculdade de Direito da Universidade de São Paulo (USP)

a doutora Madalena Teixeira disse sobre o Regulamento Europeu de Proteção de Dados (GDPR) se aplica a nós, brasileiros. Por qual razão? Porque o Regulamento não se aplica somente aos residentes da União Europeia (UE), mas também a todos os estrangeiros que tenham clientes ali residentes, subsidiárias, ou celebrem negócios com fornecedores europeus, em que seja necessário o processamento de dados colhidos no âmbito da UE. E tal utilização só é permitida desde que a jurisdição desse estrangeiro mantenha um grau de proteção aos proprietários dos dados equivalente aos outorgados pela União.

Esse mecanismo habilidoso fez com que todas as grandes diretrizes do regulamento europeu fossem exportadas para o mundo, dentre os quais o Brasil. Isso significa que a Lei Geral de Proteção de Dados no Brasil não sofreu um debate profundo na sociedade. O modelo europeu foi importado a toque de caixa, para que não houvesse a interrupção dos negócios com base em eventual desconfiância europeia de que o Brasil não protegesse os direitos dos proprietários dos dados. Em linhas gerais, nem de longe se cogitou a hipótese de que o Brasil deixasse de adotar uma regulamentação semelhante à da UE.

Este *mapa mundi* mostra, na cor azulada, os Estados que já adotaram uma legislação cuja proteção dos dados pessoais é considerada equiparável ao modelo europeu. Na cor vermelha estão indicados os Estados que sancionaram o mesmo tipo de legislação, mas que ainda não está em vigor, com é o caso brasileiro. Por fim, o mapa indica, na cor bege, as jurisdições que ainda não possuem tal iniciativa.

E o que nos chama a atenção dentre os Estados pintados de bege são justamente os Estados Unidos e a China, sem dúvida alguma os Estados em que há mais inovação relacionada à circulação de dados, inteligência artificial e desenvolvimento tecnológico do globo. Por quê?

No caso americano, eles consideram que as legislações

esparsas, no âmbito de seus estados federados, já protegem os eventuais abusos na utilização indevida de dados pessoais ou quando ocorrem os incidentes, vazamentos e ataques *hackers*.

No caso da China, a sociedade ainda não detém outros direitos fundamentais reconhecidos pelo Estado, o que faz com que as questões relacionadas às informações pessoais e privacidade não façam parte da pauta legislativa. Além disso, como a China detém o maior número de usuários de internet do mundo, com enormes conglomerados empresariais de atuação mundial, a legislação chinesa deve equilibrar o interesse dos indivíduos, das empresas e do governo, ao contrário da iniciativa da União Europeia, em que o direito à privacidade e o acesso dos usuários aos seus dados pessoais restringiram a forma como as empresas obtêm e manipulam as informações.

Diferenças culturais em relação ao temor de uso dos dados pessoais

Uma questão inicial a ser tratada se relaciona aos conflitos de cultura, tão caros ao Direito Internacional Privado. Como exemplo, temos a noção que o brasileiro em geral tem a respeito de seus dados pessoais, quando comparamos com a tradição alemã. São duas visões com-

“Outro ponto muito importante é a conexão que a LGPD faz com o macrossistema brasileiro de proteção ao consumidor (art. 18, §§ 1º e 8º), fazendo com que as faculdades e direitos presentes na lei possam ser exercitadas junto aos órgãos de proteção ao consumidor.”

pletamente distintas de mundo. Costumo comentar em aula que a primeira lei conhecida de proteção de dados pessoais surgiu na antiga Alemanha Ocidental, em 1970, no Estado de Hessen.

Durante os regimes totalitários, tanto do governo nacional-socialista do Terceiro Reich alemão, quanto na Alemanha Oriental, pela atuação da polícia secreta (Stasi), a perseguição estatal baseada no controle dos dados pessoais criou profundas cicatrizes na sociedade alemã. A administração nazista utilizou os arquivos municipais colhidos durante a República de Weimar para identificar e perseguir judeus, alguns deles por meio da busca de antepassados de até quatro gerações anteriores.

Na Alemanha Oriental, de onde a chanceler Angela Merkel é originária, o governo comunista impôs a obrigação de todas as residências disporem de um caderno de anotações, onde toda a movimentação dos moradores (entrada, saída) e visitas, deveriam ser registradas. Além disso, a paranoia dos alemães orientais quanto à possível atuação de espiões ocidentais fez com que a vigilância de vizinhos e parentes fosse incentivada à exaustão.

Aliás, quando o exército alemão ocupou os Países Baixos, encontrou em Amsterdam um relatório elaborado pela prefeitura, onde havia um banco de dados contendo a religião de todas as famílias da cidade, cujo propósito era o de fornecer eventual serviço funerário de acordo com a fé praticada pelo falecido. Com base nesse banco de dados é que a família de Anne Frank foi capturada.

Todo esse histórico opressor a respeito do uso dos dados pessoais por governos despóticos fez com que a maioria da sociedade europeia tivesse uma verdadeira repulsa a qualquer forma de acesso irrestrito aos dados pessoais que pudessem pôr em risco a privacidade da população. Trata-se de um fenômeno sociológico absolutamente justificável naquele continente.

Um exemplo prático: o Google Street View. Quem usa

a ferramenta preenche um certo endereço, sendo possível identificar, na maioria das vezes, a casa ou o prédio de destinação, assim como os imóveis vizinhos, facilitando o trajeto enormemente. Na Alemanha, mais de 90% dos proprietários solicitaram ao Google que excluísse a imagem de seus endereços dessa ferramenta. Para a maioria das famílias alemãs, a identificação de suas residências constitui uma infração à sua privacidade.

Por outro lado, no Brasil, a situação é absolutamente oposta. É muito comum que os usuários do Twitter anunciem a passagem dos carros fotográficos do Google Street View por um determinado trajeto, como forma de prevenir os transeuntes e moradores do entorno, para que possam “posar” para a ferramenta, em situações muitas vezes cômicas. O brasileiro, de modo geral, não só não se incomoda com a divulgação da fachada de sua residência, como parece, muitas vezes, apreciar tal divulgação. Pode-se dizer que, do ponto de vista sociológico, o brasileiro tradicional não tem o mesmo temor da utilização de seus dados pessoais, como o alemão.

Eu estive na Alemanha no ano passado, pesquisando durante algum tempo na Universidade de Freiburg, e pude constatar algumas ocorrências para lá de curiosas. Grosso modo, pude constatar que os universitários locais não utilizavam tanto o Facebook quanto os universitários brasileiros, nem faziam qualquer questão de serem encontrados nas redes sociais. Segundo alguns alunos me contaram, os universitários locais que possuíam uma conta no Facebook detinham, em média, cerca de 120 amigos. Comparativamente, é possível especular que, no Brasil, um estudante do ensino médio que tenha menos de 1000 amigos no Facebook pode ser considerado uma pessoa antissocial.

Outro fato curioso que eu notei entre os estudantes alemães é que seus nomes, nas redes sociais, são formados por siglas, separados por pontos ou possuem algumas letras substituídas por números, fazendo com que seja muito difícil localizá-los. No Brasil, assim que conhecemos alguma pessoa, costuma ser simples a obtenção de informações pessoais expostas pelo próprio usuário nas redes sociais.

Um fato muito comum aqui no Brasil, em qualquer compra em *shopping center*, é sermos inquiridos no momento do pagamento com solicitações de dados pessoais que nada têm a ver com a compra em si: “Você pode me informar seu CPF para atualizar o cadastro?”, “Qual é o seu endereço?”, “Qual é seu e-mail?”. Tais informações, às mais das vezes, servem para alimentar um banco de

dados que vai gerar publicidade, envio de cupons, promoções etc., que, a rigor, não causam perplexidade ou indignação do brasileiro.

A gestão dos dados pessoais e a própria compreensão do direito à privacidade no Brasil se deu, ao longo do tempo, de forma absolutamente diferente da experiência europeia, por sua vez fundada na visão alemã. Do ponto de vista empresarial e da inovação, ela se apresenta mais próxima da visão americana. Como se vê, trata-se de verdadeiros conflitos de cultura.

Eu não quero dizer com isso que o Brasil é melhor ou pior nesse tema. Em outros temas, até posso falar que somos piores, mas neste, não somos piores ou melhores do que os titulares dos dados da União Europeia. Nossas experiências foram diferentes, fazendo com que as expectativas também o sejam. São diferenças culturais que, por seu turno, levam a choques de cultura.

É a mesma coisa do que ocorre no caso da liberdade de imprensa. Os EUA consideram a imprensa livre um quarto pilar da República, sendo tolerável certa dose de difamação em prol da informação da sociedade, sendo que cabe ao eventual prejudicado provar que a notícia se deu de forma equivocada. Já no Reino Unido, a liberdade de imprensa se dá de maneira mais restritiva, havendo o dever de o órgão de imprensa provar a veracidade de sua notícia. Não me parece possível julgar o modelo americano em detrimento do modelo inglês, ou vice-versa, posto se tratar, também, de diferenças culturais que levam a choques de cultura.

Não existe inteligência artificial sem o processamento de gigantescos bancos de dados

Essas diferenças culturais e seus consequentes choques de cultura, no caso da proteção de dados, certamente levarão a consequências jurídicas também distintas.

Embora seja louvável que o proprietário controle, limite ou cesse a circulação de seus dados pessoais, parece-me que haverá momentos em que os detentores poderão justificar de forma mais abrangente a permanência dos dados, fundados em hipóteses cada vez mais abertas de legítimo interesse. A própria sociedade detém o legítimo interesse na inovação que, como se sabe, é em grande parte impulsionada pela circulação de dados pessoais.

Não existe inteligência artificial sem o processamento de gigantescos bancos de dados. Não existe um algoritmo que sozinho preveja o futuro sem olhar o passado. Quan-

do analisamos o impacto da internet 5G, que deve estar em funcionamento no Brasil talvez em 18 meses ou 24 meses, verificamos a potencialidade de circularem quantidades enormes de dados, que permitirão finalmente o surgimento da internet das coisas e novas tecnologias que nem podemos imaginar. Não se fala somente em carros autônomos, mas também aviões autônomos, como é o caso do Uber Air, um drone fabricado pela Embraer – já em fase de testes – que se parece com um transporte da franquia Star Wars.

Muitos são os exemplos de inovação, tais como as pesquisas com os relógios digitais da Apple e da Samsung, que já monitoram a saúde de seus usuários, e que poderão inclusive permitir a fabricação de medicamentos específicos e tratamentos preventivos mediante o uso de inteligência artificial, processamento de dados e comunicação com centros de saúde.

Como parece ser evidente, todas as inovações que serão trazidas a reboque do 5G pressupõem o trânsito lícito de dados pessoais.

Como afirmou a professora Madalena, o grande mote é a utilização ilícita dos dados. A LGPD tratou da privacidade como o grande fundamento jurídico da circulação de dados, punindo as empresas pelo eventual vazamento das informações sem atacar diretamente os verdadeiros responsáveis: os *hackers*. Dessa forma, a lei tratou a questão da privacidade dentro da visão e da cultura alemã.

Com o perdão da galhofa, se o Brasil dos anos 1940 era a terra de samba e pandeiro, eu poderia dizer que hoje é a terra do YouTube e do Facebook.

No próximo *chart* há um mapa da Europa mostrando em cor verde escura, os locais mapeados pelo Google Street View, em que é possível ter acesso às imagens das ruas e das casas. A mancha mais clara, ao invés, são localidades em que não foi autorizada a divulgação dessas imagens.

É possível verificar, nesse mapa, que a quase totalidade da Europa é mapeada pelo Google Street View e as imagens estão acessíveis aos usuários do produto. A grande exceção é a área que compreende a Alemanha, pelos motivos já referidos, e a Belarus (Bielorrússia), que é acusada de impor restrição a seus nacionais para o acesso aos produtos de internet e violar os valores democráticos.

Multas penalizam incidentes de vazamento de dados no Brasil e no mundo

Ao longo do tempo, desde 2016, eu tenho monitorado

a aplicação do princípio da privacidade e da proteção de dados pessoais, tanto na União Europeia quanto no Brasil, visto que desde o sancionamento da GDPR e da LGPD já se notou a busca de tutelas judiciais em ambos os espaços, visando se antecipar à vigência dessas normativas.

No Brasil, a denominação da normativa é “Lei Geral de Proteção de Dados”, o que não se adequa tecnicamente com a Lei de Introdução às Normas do Direito Brasileiro (LINDB), posto que ela não é uma lei geral, é uma lei específica. Como exemplo, continuará em vigor a Lei de Acesso à Informação. Aliás, se algum dia encontrarem um alemão, experimentem comentar que no Brasil é possível saber o salário de qualquer servidor público, pela internet, graças a uma lei que obriga todas as esferas do governo a divulgarem tais informações. Eu asseguro que o alemão protestará vigorosamente quanto à absurda violação da privacidade do agente público.

Desde 2017 é possível notar a aplicação de multas ao redor do mundo, penalizando os incidentes de vazamento de dados. Um exemplo é a multa aplicada pela autoridade americana em face do Uber, no valor de US\$ 148 milhões, pelo fato de a empresa ter negociado o “resgate” dos dados pessoais de seus clientes, que haviam sido “raptados” por um *hacker*.

Um dos primeiros casos da União Europeia de que eu tomei conhecimento foi aplicado pela autoridade nacional portuguesa, em face do pequeno Hospital do Barreiro. Segundo foi apurado, embora o hospital tivesse menos de 100 médicos residentes, cerca de 2.000 profissionais (a maioria, ex-colaboradores) tinham ainda acesso *online* aos prontuários dos pacientes. Embora não tivesse sido reportado qualquer incidente, o risco em si fora notado pelos fiscais portugueses, o que levou à aplicação da multa de 400 mil euros ao pequeno hospital, fato esse que causou consternação em toda a UE.

A normativa europeia, exportada com sucesso para todo o mundo, levanta uma importante discussão sobre os efeitos de suas sanções na inovação. No Brasil, são conhecidas as diversas ações coletivas movidas pelo Ministério Público Federal de Brasília, e por associações de defesa do consumidor, como o IDEC, antecipando a aplicação dos princípios da LGPD. Vou comentar brevemente sobre dois casos ocorridos em São Paulo.

Um deles, muito comentado na imprensa ocorreu na operação da linha verde do metrô paulistano, pela concessionária Via 4. Basicamente, um fornecedor instalou microcâmeras em frente às portas automáticas de en-

trada dos trens, monitorando, via inteligência artificial, a fisionomia dos usuários expostos às propagandas que passavam nessas portas automáticas. A ideia seria melhorar a experiência do usuário, através da verificação do impacto nas publicidades, pela captação das micro-expressões faciais dos usuários daquela linha de metrô.

É um produto inovador, baseado na coleta de dados anonimizados de milhões de usuários, mas o IDEC considerou uma infração ao direito à privacidade, na medida em que a concessionária não havia comunicado previamente os usuários.

Foi deferida a liminar, deixando a Via Quatro de utilizar a ferramenta. Aparentemente, tratou-se de uma visão muito estreita do direito à privacidade, em que não havia identificação dos usuários, nem seria possível obter sua autorização prévia. É um caso clássico em que a interpretação radical dos princípios da LGPD trabalha contra a inovação, sem um benefício concreto.

Do mesmo modo, a imprensa noticiou a propositura de uma ação semelhante, movida contra a empresa Hering, que também começou a captar microexpressões de seus consumidores, ao passarem pelos corredores das lojas e interagirem com os produtos. A ideia seria identificar, de forma automatizada, a experiência que os próprios vendedores obtêm com a prática analógica, que são os produtos que fazem mais sucesso, e o local da estante em que tais produtos deveriam ser expostos. Em resumo, tratava-se de utilização da inteligência artificial para substituir, talvez de forma mais precisa, os relatórios feitos pela equipe de vendas ao *marketing*. Novamente, a ação coletiva fez com que a Hering deixasse de usar um recurso inovador – e que dificilmente poderia causar algum dano aos usuários – que, como no exemplo anterior, utilizava imagens dos consumidores de forma anonimizada.

Já um exemplo de incidente concreto supostamente ocorreu com o Ministério da Saúde, por conta de um ataque *hacker*. Segundo um usuário do Twitter chamado “Tr3vor”, foi detectada uma vulnerabilidade no *site* do Sistema Único de Saúde (SUS), permitindo o acesso ao prontuário dos pacientes. Segundo Tr3vor, ele tentou por diversas vezes – sem sucesso – alertar as autoridades.

O que ele fez? Ele próprio subtraiu os dados de forma maciça e os publicou num *site* americano. Supostamente, o prontuário de dezenas de milhões de brasileiros, usuários do SUS, estão disponíveis na internet, sem que o governo brasileiro tenha confirmado tanto a vulnerabilidade quanto o ataque sofrido.

No próximo *chart*, vocês poderão verificar o *site* “chippyourenemiesgdpr.com”, em inglês, hospedado em um servidor do Panamá. Ele permite a qualquer pessoa, com base na GDPR da União Europeia, redigir uma notificação de 17 páginas, visando fazer com que empresas fornecedoras de bens e serviços, empregadores, órgãos governamentais etc., apresentem em até 30 dias, uma infinidade de informações e relatórios voltados ao cumprimento da GDPR, sob pena de ser formalizada uma denúncia junto às autoridades de proteção de dados.

O objetivo declarado dos responsáveis por esse *site* é o de colapsar as estruturas públicas ou privadas com pedidos de informação.

O *site* possui um *lettering* alterando as eventuais “vítimas” dessas notificações, sendo que eu dei um *print* bastante sugestivo: “você odeia seu governo?” Esse tipo de advertência serve também para nossa plateia, formada de registradores. Todos vocês podem ser notificados, no mesmo sentido das 17 páginas que eu mencionei.

Armazenamento de dados pessoais sensíveis

É importante termos em vista que os dados não estão sempre armazenados de forma eletrônica. Muitas fábricas possuem em suas plantas a famosa caixa de currículos, para que os colaboradores possam deixar a qualificação de parentes e amigos. Tais currículos muitas vezes possuem extensos dados pessoais, alguns deles sensíveis. O financeiro manuseia dados de pagamento dos funcionários, o RH lida com os funcionários que estão afastados por problemas de saúde.

Outro setor muito sensível é a portaria, em que documentos são escaneados e armazenados, juntamente com fotos dos transeuntes, em bancos de dados de empresas terceirizadas.

Em princípio todos os negócios, independentemente do tamanho, estão submetidos à fiscalização da autoridade brasileira de proteção de dados, assim como aos órgãos de proteção ao consumidor, ao Poder Judiciário e ao Ministério Público.

Interessante notar a forma como as diversas jurisdições têm lidado com as novas tecnologias, como é o caso lei francesa de reforma da justiça, de 2019. Diz o artigo 33 dessa lei: “Os dados de identidade dos magistrados e membros do judiciário não podem ser reutilizados com objetivo ou efeito de avaliar, analisar, comparar ou prever suas práticas profissionais reais ou alegadas”. Em outras palavras, o legislador francês pretendeu impedir que fossem criadas iniciativas de



inteligência artificial envolvendo a análise da jurisprudência francesa. Eu escrevi um artigo sobre esse caso, cujo título foi “O novo julgamento de Galileu”, posto que a iniciativa francesa pretendeu declarar que o sol gira em torno da Terra.

De forma totalmente contrária, o ministro Toffoli esteve no 10º encontro da AASP, em Campos do Jordão, e falou quase 50 minutos sobre como a inteligência artificial será positiva para a administração da Justiça brasileira. Com o volume de casos que nós temos, a inteligência artificial não é uma ferramenta importante, é uma ferramenta imprescindível.

É curioso o esforço francês de tentar automatizar um acesso que é disponível a todos, posto que a jurisprudência francesa continuará acessível. Ironicamente, continuará sendo possível comparar o posicionamento dos juízes franceses, se não mais por robôs, por outro tipo de mão de obra não tão qualificada, mas de uso centenário, que é o de “estagiários”.

No próximo *chart* eu trago o *site* americano denominado “Public Record Search Service”. O usuário, ao preencher o nome, sobrenome, algum endereço, o *site* me traz as informações disponíveis em bancos de dados públicos dentro dos 50 estados federados americanos.

No Brasil, há vários *sites* semelhantes, tais como o “consultacnpj.com”, que é hospedado num servidor localizado nos EUA. Basta preencher o CNPJ que o *site* informa os dados pessoais dos sócios, de ex-sócios e dos dirigentes.

Um dos problemas derivados desses *sites*, no Brasil, é o fato dessas informações levarem a possíveis fraudes.

Compra de créditos de consumidores para propor ações massificadas

Outra nova realidade aparentemente nociva é a invasão de empresas que utilizam inteligência artificial para comprar créditos de consumidores brasileiros e proporem ações massificadas, como tem ocorrido contra o mercado de aviação civil. É possível interligar as informações de atrasos e cancelamentos de voos junto à IATA, e focar maciçamente na propaganda em redes sociais, visando à compra, por valores baixos, de expectativas de direito de eventuais passageiros impactados, aumentando exponencialmente a litigiosidade e o custo Brasil. Tais empresas, muitas delas de capital estrangeiro e travestidas do pomposo título de “civic techs”, nada mais são do que fundos abutres de compra de expectativas de crédito.

Atualmente, cerca de 10% do volume de ações consumeristas movidas contra empresas aéreas, e quase 15% das movidas contra empresas de turismo, são originadas por 30 *civic techs* das mais diversas origens, desde Hong Kong, EUA e Reino Unido. Tais iniciativas contrariam tudo o que se consolidou sobre desjudicialização, métodos adequados de solução de controvérsias e tudo mais.

O próprio conceito de dados pessoais é constantemente alargado, na medida em que a tecnologia permite a individualização da pessoa natural por intermédio de informações aparentemente aleatórias, como se vê pelos *softwares* de reconhecimento facial.

Outro ponto muito importante é a conexão que a LGPD faz com o macrosistema brasileiro de proteção ao consumidor (art. 18, §§ 1º e 8º), fazendo com que as faculdades e direitos presentes na lei possam ser exercitadas junto aos órgãos de proteção ao consumidor. Frente às empresas, o titular dos dados passa a ser a parte hipossuficiente, podendo ocorrer a inversão do ônus da prova nas futuras discussões.

Importante mencionar que o art. 42 da LGPD equipara o controlador e o operador como corresponsáveis por eventual dano patrimonial, moral, individual ou coletivo, independentemente da instauração do incidente de desconconsideração da personalidade jurídica. Tal equação, absolutamente mortífera, faz com que um incidente de vazamento de dados gere um contencioso de massa consumerista, envolvendo a necessidade da presença física do controlador ou do individual, em juizados especiais cíveis em todo o país.

Estou chamando a atenção para uma futura onda tsunâmica, envolvendo Procons, juizados, inversão do ônus

da prova e outros temas, a serem discutidos nos foros localizados no domicílio do reclamante.

Em síntese, há uma possibilidade de que esses novos atores, travestidos de *civic techs*, financiem uma iniciativa que desconside a atividade do encarregado, partindo diretamente para a judicialização em massa de eventuais incidentes de vazamentos de dados, posto que há uma legislação protetiva de padrão alemão inserido numa cultura altamente contenciosa, que é a brasileira.

Todas essas situações devem ser incorporadas pelas empresas num nível de governança equivalente às políticas de proteção ambiental, segurança do trabalho ou anticorrupção, haja vista o enorme potencial de risco financeiro que representam.

Concepção de negócios e produtos deve considerar a proteção de dados pessoais e o direito à privacidade

A LGPD impõe o dever de todas as organizações relatarem certos tipos de violação de dados pessoais à autoridade nacional de proteção de dados no menor prazo possível. E se a violação resultar em alto risco de afetar os direitos e liberdades dos indivíduos, estes devem ser comunicados o mais brevemente possível. Aí entra a necessidade premente de garantir a existência de procedimentos robustos de detecção de violações, investigação e relatórios internos. Também passa a ser necessária a manutenção de um registro de qualquer violação de dados pessoais, independentemente da obrigatoriedade de notificação da autoridade e do proprietário dos dados.

Doravante, a concepção de negócios e produtos deve necessariamente levar em conta a proteção dos dados pessoais e o direito à privacidade, no famoso conceito do *privacy by design*.

Embora a doutrina brasileira esteja focada principalmente no consentimento como a razão primária para o tratamento de dados, é importante analisar todas as possibilidades que a LGPD determina, tais como o legítimo interesse.

Em referência direta aos associados da Anoreg, importante estudar o tratamento de dados pela existência de obrigação legal, em comparação com eventuais questionamentos dos proprietários que pretenderão que cesse o tratamento de seus dados, com base equivocada em seu consentimento.

Da mesma forma, como dito, a questão do legítimo interesse no tratamento dos dados, em contraposição ao consentimento do proprietário, será de vital importância

na continuidade da evolução tecnológica brasileira, e neste ponto eu chamo a atenção dos magistrados presentes neste evento.

O conceito de legítimo interesse como base legal para o processamento dos dados está previsto no art. 7º, inc. IX da LGPD, e leva em conta, inclusive, os interesses legítimos de terceiros, incluindo benefícios mais amplos para a sociedade.

O grande desafio das empresas será o de documentar as decisões fundadas sobre os interesses legítimos, visando demonstrar a conformidade com o novo princípio de responsabilidade da LGPD.

O que é “legítimo interesse”?

A LGPD não define seu conceito, e o artigo 6 (1) (f) da GDPR é gongórico: “O processamento é necessário para fins dos interesses legítimos perseguidos pelo responsável pelo tratamento ou por terceiros, exceto quando esses interesses forem substituídos pelos interesses ou direitos e liberdades fundamentais do titular dos dados que exijam proteção de dados pessoais, em particular quando os dados sujeito é uma criança.”

Em linhas gerais, o tratamento de dados com base no legítimo interesse é considerado, na experiência da União Europeia, após ultrapassar um teste de três partes:

1. Teste de objetivo: a empresa, no tratamento desses dados, está buscando um interesse realmente legítimo?

2. Teste de necessidade: o processamento é necessário para esse fim?

3. Teste de equilíbrio: os interesses do indivíduo substituem o interesse legítimo?

Uma ampla gama de interesses pode ser legítima. Eles podem ser os próprios interesses da empresa ou de terceiros, interesses comerciais e benefícios sociais mais amplos. Eles podem ser convincentes ou triviais, mas interesses triviais podem ser mais facilmente substituídos no teste de balanceamento.

A LGPD sugere o uso de dados de clientes ou funcionários, *marketing*, prevenção de fraudes, transferências intragrupo ou segurança de TI como possíveis interesses legítimos, mas essa não é uma lista exaustiva. A norma também reconhece o interesse legítimo em divulgar informações sobre possíveis atos criminosos às autoridades.

O processamento deve ser considerado uma maneira proporcional de atingir o objetivo.

Em linhas gerais, caberá à autoridade nacional de proteção de dados e aos magistrados brasileiros definir

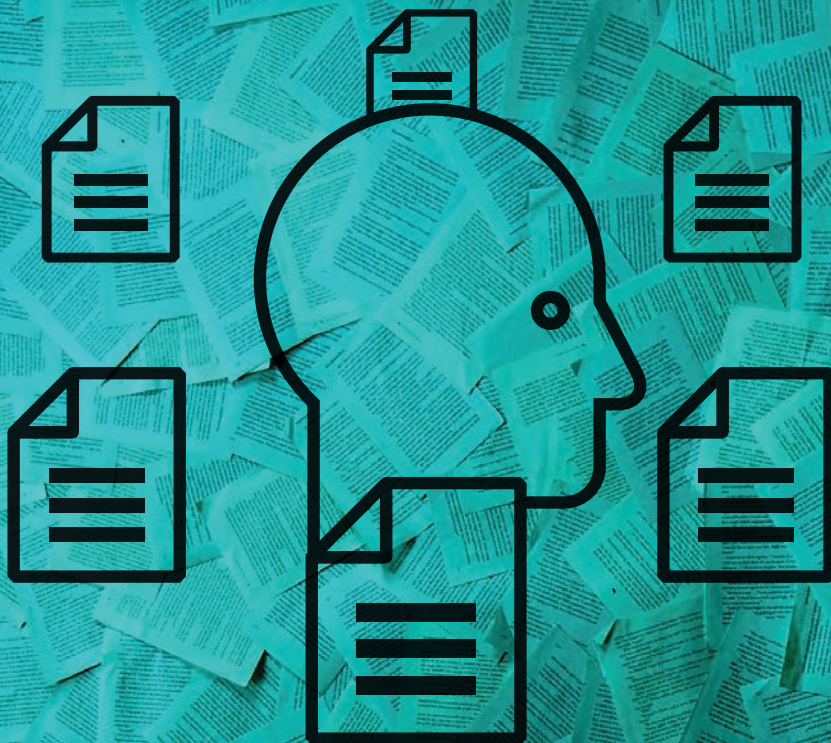
os limites do legítimo interesse. Eu tenho a expectativa, para não dizer convicção – pois esse tem sido o objeto dos meus estudos –, de que a utilização dos dados fundada no legítimo interesse não seguirá a visão restritiva alemã, haja vista as peculiaridades da cultura brasileira, hoje fonte de inovação positiva.

Como afirmou a revista *The Economist*, dados são o novo petróleo. Eu ouvi de um professor alemão que se dados são o novo petróleo, então temos que achar um jeito de tributá-los. Esse não parece ser o pensamento que fundamenta a inovação. De qualquer forma, sem querer deturpar o conceito de legítimo interesse, a inovação só vai existir, no que diz respeito à inteligência artificial, por conta do trânsito responsável dos dados.

Toda nova tecnologia gera impactos, nem todos positivos. Isso aconteceu quando Thomas Edison inventou o primeiro fonógrafo e tentou gravar um concerto em Nova York. Ele foi expulso do recinto a pontapés. O maestro, à época, achava que aquele invento poderia acabar com a sua profissão, tornando-o obsoleto.

Convidando-os para essa reflexão, aqui eu encerro minha participação neste painel, deixando também o convite para acessarem o *site* mantido por meu escritório, onde são direcionadas diversas novidades, artigos, jurisprudências etc., chamado “lgpdbrasil.com.br”.





Lei Geral de Proteção de Dados – uma aproximação aos conceitos da lei



1. Perspectivas e



BRUNO RICARDO BIONI

Advogado e professor na área de regulação e novas tecnologias, com especialidade na área de proteção de dados pessoais. Doutorando e mestre em direito pela Universidade de São Paulo (USP).

impactos da LGPD no Brasil

Hoje eu pensei em falar um pouco de perspectivas e impactos da Lei Geral de Proteção de Dados Pessoais no Brasil, e aí já vai um pouco dos conceitos básicos e elementares.

O que é a LGPD, o que é Lei Geral de Proteção de Dados Pessoais, e qual é o seu impacto regulatório, inclusive econômico. É com isso que vamos estar preocupados quando essa lei entrar em vigor.

Na segunda parte vamos falar um pouco mais de conceitos básicos, do elemento-chave, do que é o dado pessoal. O que essa lei abraça, o que está debaixo do guarda-chuva dela. A lei trouxe várias hipóteses, várias bases legais, e eu vou tratar mais de perto duas delas que acho que são as duas principais, o legítimo interesse e o consentimento. E aí eu vou falar das figuras dos agentes do tratamento de dados pessoais, e por último eu fecho com algumas tendências.

1.1 O que é a Lei Geral de Proteção de Dados – LGPD?

O que é a Lei Geral de Proteção de Dados Pessoais? Eu acho que vale a pena trabalhar com esse adjetivo, que é chave: geral, transversal, aquilo que complementa, por assim dizer, um quebra-cabeça que a gente já tem no Brasil em termos de normas sobre proteção de dados pessoais.

É equivocado dizer que antes da LGPD tínhamos um completo vazio regulatório, porque havia muitas leis setoriais tratando da matéria. Nós vamos encontrar isso no Código de Defesa do Consumidor, com os dispositivos específicos que regulam bancos de dados; na Lei do Cadastro Positivo, que trata da matéria do ponto de vista de concessão ao crédito; e até na Lei de Registros Públicos quando ela trata de questões de confidencialidade, de quem são as partes legalmente habilitadas para consultar determinados dados pessoais ali previstos em determinadas matrículas, em determinados registros, e assim por diante.

Nós temos uma colcha de retalhos sobre proteção de dados pessoais, e esse era o grande drama no Brasil, porque nenhuma dessas leis foi concebida para tratar única e exclusivamente de proteção de dados pessoais.

Por exemplo, no Código de Defesa do Consumidor há três dispositivos que vão tratar da matéria. O Marco

Civil da Internet vai tratar de neutralidade da rede, de remoção de conteúdo. Ou seja, nenhuma dessas leis é vocacionada para tratar da matéria de proteção de dados pessoais.

Esse é o ponto principal dessa nova peça desse quebra-cabeça regulatório. Por quê? Porque temos uma lei que, do início ao fim, procura endereçar, tratar a matéria, ela vai nos fornecer o vocabulário básico para podermos dialogar sobre proteção de dados pessoais no Brasil. E esse impacto é superpositivo.

Nesta tabelinha temos aquelas leis setoriais que eu destaquei: o Código de Defesa do Consumidor, Marco Civil da Internet, o decreto do Marco Civil da Internet, a Lei do Cadastro Positivo, e a Lei de Acesso à Informação.

Todas essas leis tratam, em menor ou maior medida, sobre proteção de dados pessoais. Todas elas têm algum dispositivo para falar de proteção de dados pessoais.

No entanto, pelo menos até 2011, quando foi editada a Lei de Acesso à Informação, não tínhamos o conceito básico para falar de proteção de dados pessoais, o conceito de dado pessoal. O que aqueles dispositivos do Código de Defesa do Consumidor procuram tutelar, por assim dizer? O que o Marco Civil da Internet, até a edição do seu decreto de Marco Civil da Internet, procurava proteger? Havia vários dispositivos ali procurando governar a matéria, mas não havia o conceito básico para se falar de qualquer dado efetivamente protegido, abraçado por essas regras.

No Brasil havia não um vácuo regulatório, mas um problema de regulação no sentido de que não tínhamos todos os conceitos, o vocabulário básico para falar de proteção de dados pessoais.

Agora, com a Lei Geral de Proteção de Dados Pessoais, vamos ter as definições básicas, desde o conceito de dado pessoal, o que é tratamento de dados pessoais, aquela definição ampla.

Há mais de vinte operações, mais de vinte atividades, mais de vinte verbos definindo tratamento de dados. É da coleta ao descarte. Isso vai estar previsto na nossa lei, todos os princípios básicos para se tratar da matéria. Princípio da finalidade, por exemplo, você tem que especificar o propósito para o qual você está coletando, tratando um dado.

Acabou aquele negócio de políticas de privacidade pedirem os seus dados para melhorar a sua experiência. Que finalidade é essa? Não especifica nada, não tem um propósito bem ilustrado. É essa a ideia do princípio da finalidade. Colocar esse dever, esse ônus nos ombros das entidades que tratam dados pessoais para ter uma relação mais sincera, mais transparente. E esse é outro princípio que também vai estar na nossa Lei Geral de Proteção de Dados Pessoais.

1.2. Os impactos regulatório e econômico da LGPD

Tudo isso para dizer que nossa Lei Geral de Proteção de Dados Pessoais acabou tendo bastante apoio e, principalmente, tração no Congresso Nacional, por conta deste aspecto: vamos ter uma nova peça no nosso quebra-cabeça regulatório, que vai trazer segurança jurídica. É esse o grande jargão que se usou para que essa lei fosse aprovada rapidamente antes do novo pleito eleitoral, não só por agentes econômicos, mas eu diria pela sociedade civil brasileira como um todo.

É muito simbólico olhar para o processo da LGPD e ver uma verdadeira coalizão de vários setores da organização: academia, terceiro setor, ONGs, setor privado e até, em determinado sentido, alguns membros do próprio governo. Por quê? Porque a falta de segurança jurídica era ruim para todo mundo. Era ruim para o gestor público, que iria tratar dado pessoal e não tinha ali todos os conceitos para poder formular uma política pública baseada em dados. Era ruim para o setor privado, que não tinha ali todos os conceitos para saber quais eram os limites, as possibilidades de pensar um serviço, um aplicativo, um produto e assim por diante. Era ruim para o cidadão também, porque ele não tinha ali todos os seus direitos assegurados, prescritos e todo um conjunto de regras para governar e estabelecer essa relação de forma um pouco mais equilibrada.

Então, quando falamos propriamente de aproximar conceitos, é muito importante sinalizar na alma dessa Lei Geral de Proteção de Dados Pessoais, que ela tenha uma dupla função. Ela vem para, nos seus fundamentos, não só fomentar o desenvolvimento econômico e tecnológico, mas também proteger direitos e liberdades fundamentais.

Aliás, toda e qualquer regulação deve ter esses efeitos colaterais positivos, por assim dizer, tanto por parte de quem é o vulnerável a ser tutelado naquela relação, quanto do ponto de vista de quem é a parte mais forte

que precisa saber quais são os limites e as possibilidades para poder escorar suas atividades com base nisso.

Estou procurando trazer isso de volta porque já se passou um ano desde que a lei foi sancionada e ainda percebemos um verdadeiro terrorismo, muito medo de que a lei prejudique as atividades do gestor público ou inviabilize vários modelos de negócio. Não, a ideia dessa lei, por conta justamente dessa dupla função, é trazer segurança jurídica para todo mundo, e isso envolve, inclusive, quem exerce atividade econômica baseada em dados.

E o melhor exemplo disso é o caso de modernização dessa regulação na União Europeia. O Regulamento Europeu de Proteção de Dados Pessoais – GDPR, inspirou muito a nossa Lei Geral de Proteção de Dados.

Esse regulamento entrou em vigor em 2018, mas foi aprovado em 2016, teve dois anos de *vacatio legis* até entrar em vigor. Dois anos para poderem se adaptar, tanto o setor público quanto o setor privado. Quando se olha para a experiência acumulada desses dois anos de um processo de conformidade, ou de vários processos de conformidade, o que se percebe é que aquelas organizações que usaram esse tempo como uma janela de oportunidades, entendendo que a lei não era para inviabilizar suas atividades, mas justamente para ajudar as suas atividades, encontraram, nessa regulação, uma grande força motriz para organizar os seus processos, para arrumar a casa, por assim dizer.

Essa nova regulação forçou as organizações a criarem ordem na informação que elas tinham. E essa ordem gerou valor, gerou *insight*, ideias em algo que estava sendo subutilizado ou que estava, de certa forma, escondido.

Eu sempre costumo trazer a metáfora de começarmos a pensar esse processo de conformidade da LGPD mais ou menos como enxergamos o nosso guarda-roupa em casa.

Todo mundo já teve o guarda-roupa desarrumado um dia. É horrível, não é? Por quê? Porque você abre o seu guarda-roupa e vê todas as suas roupas desorganizadas, todos os dados não catalogados, e você demora muito mais tempo para tomar a decisão de qual roupa usar.

Hoje, graças a Deus, o meu guarda-roupa está bem arrumado, eu consegui colocar o meu terno para vir aqui, escolhi a minha gravata para vir aqui dar aula. Se eu fosse para a academia, iria utilizar outra roupa completamente diferente. Mas é essa a ideia, e ela é muito importante. Sejam vocês enquanto parte do Poder Judiciário, sejam vocês enquanto membros de cartórios, registradores,

“É uma lei geral de proteção de dados pessoais, com todo o vocabulário básico para falarmos da proteção de dados pessoais no Brasil, e isso vai nos ajudar enquanto organizações a arrumar a casa, a arrumar o nosso guarda-roupa de dados.”

registradoras. É a oportunidade de olhar para essa lei, para essa nova regulação, e organizar os processos que existem dentro das organizações de vocês. E a partir disso, digamos assim, fazer desse limão uma limonada, olhar para o que diz a Lei Geral de Proteção de Dados Pessoais. Você precisa saber qual dado você tem dentro da sua organização, quem tem acesso àquele dado dentro da organização, e quando aquele dado já não é mais útil para a sua organização.

Tudo isso vai gerar uma história para esse dado, para essa informação. Você vai conseguir enxergar valor, vai conseguir gerar mais eficiência para os seus processos e assim por diante. Eu acho que essa é uma primeira ideia para aproximar conceitos e para desmistificar algumas ideias que têm sido passadas com relação a essa Lei. Ou seja, vamos olhar para essa nova regulação não do ponto de vista do aspecto negativo, mas do aspecto positivo. E no final eu volto a trabalhar essa ideia do que deve ser uma jornada de um processo de conformidade.

Mas antes disso, eu acho que vale a pena reprisar duas coisas: é uma lei geral de proteção de dados pessoais, com todo o vocabulário básico para falarmos da proteção de dados pessoais no Brasil, e isso vai nos ajudar enquanto organizações a arrumar a casa, a arrumar o nosso guarda-roupa de dados.

2. Conceitos básicos na LGPD

Entendemos, então, aquela primeira parte da lei, muito importante, que são os fundamentos da Lei Geral de Proteção de Dados Pessoais. Ela fala dessa dupla função: fomenta o desenvolvimento tecnológico, econômico, livre desenvolvimento da personalidade das pessoas, ou seja, procura balancear as duas partes desse processo.

Ela vai avançar nos seus artigos e começar a conceituar aquilo que veio para regular, aquilo que está dentro do seu escopo de aplicação, aquilo que está debaixo da sua asa, que está debaixo do seu guarda-chuva. Ou seja, o que é dado pessoal.

2.1. Delimitando o escopo da LGPD:

o conceito de dado pessoal

A lei não veio para regular qualquer tipo de dado, ela veio para abraçar aquilo que é dado pessoal, dado de pessoa natural, se você quiser, pessoa física. Dados de pessoa jurídica vão ter outro regramento, vão ter outro regulamento muito mais associado à questão de propriedade intelectual, sigilo industrial, e assim por diante. Mas os dados relacionados a pessoas naturais, a pessoas físicas, são sim acobertados e protegidos por essa lei.

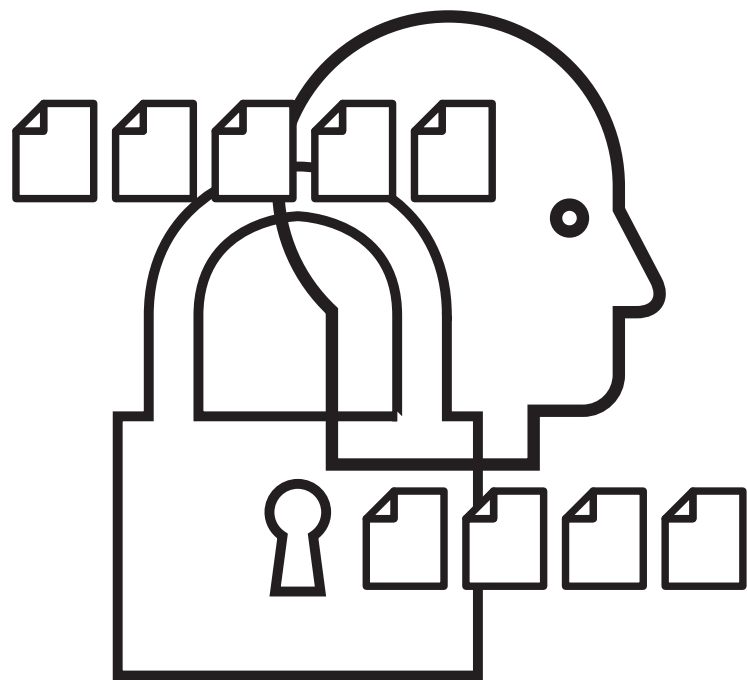
Começamos, então, a falar dos conceitos básicos. Primeira coisa que eu gostaria de destacar aqui é que os dados não deixam de ser pessoais por serem de titularidade do seu colaborador ou da sua colaboradora.

Então, essa lei vai ter impacto para muito além do que somente relações de consumo. Até mesmo relações de trabalho vão ter que ser reinterpretadas, tem que ser feita uma releitura do que é essa nova carga protetiva em cima do titular daquela informação.

Muitas vezes pensamos em processo de conformidade do ponto de vista do *business*, daquilo que a nossa organização faz. Por exemplo, os cartórios, que tratam uma quantidade enorme de dados pessoais, mas temos que pensar que a lei é muito mais impactante do que isso. Ela vai olhar para você enquanto organização, enquanto um fiduciário de informação, até mesmo dos seus colaboradores e colaboradoras.

Então é uma lei que tem impacto muito forte, transversal, por isso Lei Geral de Proteção de Dados Pessoais, e que vai alcançar até mesmo as relações trabalhistas de maneira geral.

Outra ideia equivocada é que a LGPD seria uma lei que apenas protegeria dados pessoais tratados por empresas de tecnologia ou por empresas que têm modelos de negócios na internet. Olha lá o adjetivo-chave, geral. É uma Lei Geral de Proteção de Dados Pessoais. Pouco importa se você está coletando esse dado numa folha de papel ou num aplicativo no seu *smartphone*. A lei abraça tudo aquilo que é dado pessoal, não importa o meio



no qual você está coletando, processando ou tratando dados pessoais.

O âmbito de aplicação da LGPD vai, portanto, muito além do próprio setor privado, alcançando também, como eu falei aqui, o setor público. Alcança registradores, registradoras, cartórios. O adjetivo-chave, mais uma vez, é uma Lei Geral de Proteção de Dados Pessoais.

O dado do meu colaborador, eu vou ter que reavaliar como eu coeto. Como eu faço folha de pagamento? Serão necessários todos aqueles dados? Como eu vou repassar os dados do meu colaborador e também dos dependentes dele para o plano de saúde? Eu vou ter que rever até isso, para além do meu *call business*, seja lá qual for a entidade ou organização.

Além disso, a Lei Geral de Proteção de Dados Pessoais também prescreveu o “conceito expansionista de dado pessoal”, um conceito abrangente de dado pessoal. É uma informação relacionada a uma pessoa identificada ou identificável. E esse termo, identificável, é que é o problema. Porque a partir dessa concepção de que o conceito de dado pessoal é mais alargado, ele vai muito além do número de RG, do número de CPF ou da biometria. É toda e qualquer informação que nos possa identificar.

Vamos pensar em portais, ou aplicações da internet, com aqueles pequenos rastreadores que ficam monitorando tudo o que o usuário faz. Eu não sei necessariamente que é o Bruno que está por trás daquele dispositivo, mas ele visitou o *site* da EPM, depois visitou o *site* da Globo. Eu vou coletando várias informações que, uma vez agregadas, podem vir a formar esse quebra-cabeça ou a identidade do Bruno.

Portanto, o que precisamos compreender a respeito da LGPD é que o conceito de dado pessoal é muito mais do que o nosso RG, do que o nosso CPF, do que a nossa biometria. Basta vocês pensarem na própria atividade de vocês enquanto cartórios. Vocês têm uma grande quantidade de informações que não necessariamente se referem sempre a esses dados de RG e CPF, mas a uma série de composições de informações que vão permitir identificar outras pessoas ou mesmo aquelas pessoas que estão ali literalmente identificadas numa matrícula de imóvel, por exemplo.

Então, essa é uma mensagem que eu gostaria de passar para aproximarmos conceitos: a LGPD é uma Lei que vai olhar para o dado do ponto de vista mais abrangente, relacionado a uma pessoa identificada ou identificável.

Há um segundo aspecto que eu gostaria de tratar com vocês, ainda referente a conceitos básicos.

A lei procurou criar quase que uma taxonomia do que seja dado pessoal. Ela criou, por assim dizer, uma primeira espécie de dado – que seria aquela ideia de um dado normal, um dado trivial – e uma outra categoria de dado, que seria um dado um pouco mais sensível, ou seja, aquilo que teria um risco maior para o próprio titular, por exemplo, de ele poder sofrer determinados tipos de práticas discriminatórias. Essa é a ideia de dado sensível. Dado relacionado ao seu estado de saúde, questões genéticas, biometria, orientação político-partidária, religiosa. Tudo isso é dado pessoal, mas é dado pessoal sensível.

A lei fez essa bipartição, esse partilhamento, para criar dois regimes jurídicos distintos. Consequentemente, naquilo que é dado normal, trivial, o regime jurídico é um pouco mais relaxado, um pouco mais brando. Quando se trata de dado pessoal, sensível, o regime jurídico é mais protetivo.

E, realmente, as obrigações são muito maiores em torno daquelas organizações que tratam dados sensíveis.

Outro ponto importante. A LGPD procurou dar também tratamento mais protetivo mesmo tratando-se de dados triviais, mas a agregação desses dados leva a informações sensíveis sobre o indivíduo.

No universo de cartórios, muitas vezes as informações registradas possibilitam, eventualmente, chegar em inferências sensíveis sobre determinada pessoa. Então, esse é outro recorte que vocês terão que imaginar.

É uma questão de olhar para as atividades e, eventualmente, pensar se você visa fazer alguma inferência sensível daquela pessoa. Se você não visa, deixe isso

claro, porque aí você está em outro regime jurídico completamente distinto daquele.

2.2. Delimitando o escopo da LGPD: o conceito de dado anonimizado

Dito isso, a lei traz outro conceito muito importante, o outro lado da moeda, aquilo que não estaria debaixo do guarda-chuva dela, a ideia de dado anonimizado, ou dado anônimo. A definição no dicionário é que dado anônimo é aquilo que não tem cara e nem rosto, portanto, não identifica um sujeito. É isso que a lei procura trabalhar, essas duas ideias.

A LGPD trouxe o conceito explicitando o seguinte: para verificar se um dado é efetivamente anônimo ou anonimizado, é preciso levar em consideração alguns critérios, alguns fatores objetivos, para saber se esse dado não pode vir a identificar um sujeito, ou um titular, ou uma pessoa.

A lei colocou três fatores: custo, tempo e estado da arte e da tecnologia. Por exemplo, a Lei de Acesso à Informação traz bastantes políticas de dados abertos. Então, vários gestores públicos federais, estaduais ou municipais têm essa boa prática de abrir dados. Eles procuram não identificar o cidadão, mas ao abrir esses dados acabam gerando o risco de que esses dados sejam cruzados com outros e venham a compor esse efeito mosaico de informação.

Por isso, a própria LGPD procura trazer esse ponto de reflexão, como os gestores públicos devem pensar em abrir dados sem abrir a privacidade das pessoas ou a proteção de seus dados. E para não indicar qual seria a melhor tecnologia para abrir dados ou para anonimizar dados, a lei criou esses conceitos um pouco mais abertos que são: custo, tempo e estado da arte.

Vou dar outro exemplo. Hoje, começamos a falar de computação quântica. Isso provavelmente vai ser uma realidade daqui a X anos. Não sabemos ao certo o que é, mas provavelmente vai mudar o estado da arte da tecnologia, esse o termo utilizado pela lei. O estado da arte da tecnologia, ou seja, as tecnologias disponíveis pelas quais poderemos cruzar dados, aumentar a qualidade e a quantidade de processamento de informações e – com menos custos, menos tempo –, cruzar mais bases de dados e identificar mais facilmente um determinado sujeito.

A LGPD foi neutra em termos tecnológicos. Então esses conceitos, esses fatores objetivos para se saber o que é efetivamente um dado anonimizado vão ser calibrados de acordo com as tecnologias disponíveis. E a

partir dessas tecnologias disponíveis, qual é o tempo, o custo para se agregar informações anonimizadas e vir a identificar uma pessoa, para então eu cair na malha fina do conceito de dado pessoal.

Então, essa é outra definição importante que a lei traz. Ao mesmo tempo, ela inova no ordenamento jurídico brasileiro, porque não tínhamos esse conceito de dado anonimizado. Então, ao mesmo tempo que ela traz o conceito de dado pessoal alargado, expansionista, ela procura fechar o âmbito e o escopo de aplicação trazendo aquilo que está fora dos tentáculos dela, por assim dizer.

2.3. Delimitando o escopo da LGPD: *profiling*

A lei procura trazer a ideia de perfilamento ou *profiling*.

Quando se tem uma atividade em que se monitora, se acompanha uma pessoa, ou um indivíduo, e se consegue gerar dados, inferências sobre o comportamento dessa pessoa, essa é uma atividade de alto risco para os direitos e liberdades fundamentais do titular. Então, a LGPD procurou dar um regime um pouco mais protetivo para o indivíduo.

Quando você está fazendo um exercício de perfilamento, um *profiling*, e você automatiza decisões que vão ser tomadas com base naquele perfil comportamental formado, você tem outros direitos, direitos a mais por parte do titular para que ele possa sair, por assim dizer, desse julgamento, ou pelo menos para que ele possa entender qual é o julgamento que está sendo feito sobre ele.

Quem aqui já pediu crédito no banco? Hoje funciona a partir principalmente de notas, o chamado *credit scoring*. Um perfil comportamental meu, do Bruno. Não só eventualmente das contas que eu deixei de pagar, mas também das contas que eu paguei em dia com maior ou menor pontualidade. Tudo isso vai formando um perfil comportamental meu, do Bruno, com relação à minha capacidade socioeconômica, minha capacidade de pagar minhas contas. E com base nisso é feita uma nota minha que vai dizer: 1) se eu sou elegível ou não para determinada linha de crédito; 2) se, sendo elegível, eu tenho maior ou menor risco, e a minha taxa de juros vai ser maior ou menor.

Em várias situações estamos em circuitos decisórios automatizados. A LGPD procurou dar outros direitos para o titular. Por exemplo, eu quero saber a lógica pela qual esse algoritmo, ou esse computador, está decidindo a minha nota. Eu quero o meu direito à explicação. Se eu acho que não me enquadro como alto risco, como mau pagador, eu quero que seja revisada a decisão tomada

por essa máquina. Eu quero ter o direito de revisão dessa decisão automatizada.

Ao mesmo tempo, a lei procurou olhar para situações nas quais o tratamento de dados pessoais poderia representar um risco para direitos e liberdades fundamentais das pessoas, e garantir novos direitos, para que o indivíduo possa saber como ele é olhado, enxergado e julgado numa sociedade cada vez mais movida e orientada por dados. Esse é outro conceito importante da nossa Lei Geral de Proteção de Dados Pessoais.

2.4. Dados públicos e dados publicamente acessíveis: um diálogo entre o direito à privacidade e o direito à proteção de dados pessoais

Há outro conceito que eu gostaria de trabalhar, principalmente porque a atividade de vocês é tornar dados públicos, ou pelo menos acessíveis publicamente, por parte das pessoas que querem saber quem é o titular, o proprietário de um imóvel, qual a data de nascimento de uma pessoa, a filiação etc.

A Lei Geral de Proteção de Dados Pessoais vem para, de certa maneira, mudar nossa mentalidade com relação ao direito à privacidade. E ela muda mesmo ao estabelecer que direito à privacidade é uma coisa, direito à proteção de dados pessoais é outra coisa. Nós precisamos entender esse conceito para não cair em algumas armadilhas da LGPD.

Qual é a diferença, então, entre o direito à privacidade e a proteção de dados pessoais? Não são a mesma coisa? Não, não são.

O direito à privacidade trabalha muito naquela lógica de uma liberdade negativa, ou seja, sair de um espaço público, ou semipúblico, e ir para a própria casa, onde o espaço é privado e onde se tem uma série de garantias. Garantias constitucionais da inviolabilidade do domicílio, e assim por diante. É uma liberdade negativa; eu saio da esfera pública e me coloco a salvo. Trabalha muito nessa lógica dicotômica, binária, do público e do privado.

O direito à proteção de dados pessoais é completamente diferente. Em vez de uma liberdade negativa, é uma liberdade positiva no sentido de eu controlar as minhas informações, os meus dados. Pouco importa se esses dados são públicos ou são privados. Pouco importa se essas informações são captadas numa praça pública ou se elas são captadas no meu prontuário médico. O dado público, ou de acesso público, não deixa de ser dado pessoal.

E isso é uma coisa que temos que trabalhar no Brasil

porque já vimos alguns precedentes, inclusive decisões judiciais, flexibilizando o grau de proteção de dados pessoais por eles serem públicos ou publicamente acessíveis. A Lei Geral de Proteção de Dados Pessoais vai quebrar esse raciocínio.

Para não deixar dúvidas sobre isso, a lei foi pedagógica. A definição de dados públicos, ou dados manifestamente públicos, (§ 7º do art. 7º), diz com todas as letras que o dado pode estar numa base publicamente acessível, mas nem por isso você pode fazer qualquer coisa com ele. Você tem que verificar qual foi a finalidade pela qual ele foi publicizado e se o tratamento que você vai dar para esse dado está vinculado àquela finalidade inicial para a qual ele foi publicizado.

Um exemplo é a criação de perfis no LinkedIn. Esses dados são publicizados, tornados públicos por nós mesmos, os titulares, para sermos notados por eventuais novos empregadores ou por profissionais da nossa comunidade. Como funciona hoje o processo seletivo? Uma empresa de *headhunter* cria um robzinho para varrer perfis no LinkedIn e descobrir profissionais com um perfil associado à demanda daquela posição. O que essa empresa faz? Ele trata dados pessoais, publicamente acessíveis, mas leva em consideração a finalidade para a qual aquelas pessoas publicizaram seus dados. Portanto, essa empresa está super de acordo com a Lei Geral de Proteção de Dados Pessoais. A Lei não veio para inviabilizar o modelo de negócio dela, veio, inclusive, para viabilizar o modelo de negócios dela. Imagine se a empresa de *headhunter* tivesse que sair pedindo o consentimento de todo mundo do *LinkedIn*!

Ao mesmo tempo, existem vários outros modelos de negócios, ou outras atividades, que não levam em conta esse contexto pelo qual esse dado foi publicizado. Podemos pensar em outros exemplos reais, como, por exemplo, da indústria de *data brokers*, ou os *bureaus* de crédito. Algumas empresas também fazem raspagem dessas bases de dados públicas para saber se a pessoa tem maior ou menor potencial inadimplente ou adquirente, para então calcular a sua nota de risco. Por exemplo, é possível descobrir, no LinkedIn, que alguém troca de emprego a cada cinco ou seis meses. Qual é a inferência que se pode fazer? Que essa pessoa tem instabilidade financeira e, a partir desses dados pessoais publicamente acessíveis, gerar uma nota negativa sobre ela.

Por isso, a LGPD diz que deve ser considerada a finalidade pela qual a pessoa publicizou seus dados. Ao publicar seus dados no *LinkedIn* será que essa pessoa

“Pouco importa se o dado é público ou privado, o que importa é a finalidade pela qual ele foi processado e está sendo publicizado. Isso vai gerar uma mudança na nossa cultura jurídico-legal brasileira. E isso está na LGPD.”

esperava que eles fossem compor a sua nota de crédito? A lei procura quebrar essa dicotomia enraizada no campo do direito à privacidade para trabalharmos com outra lógica, com outra dinâmica, no campo de proteção de dados pessoais.

Isso significa que os *bureaus* de crédito e os *data brokers* vão ter que parar com qualquer tipo de raspagem de dados públicos? Não. Por que tornamos vários processos judiciais públicos, principalmente olhando para questões de anulabilidade de negócios jurídicos, e para fraude à execução? São dados publicamente acessíveis. Ao comprar um imóvel eu tenho que verificar se não há uma ação judicial que pode levá-lo à insolvência ou se seria fraude à execução. Qual é a finalidade pela qual esse dado é público? Não é justamente para trazer maior segurança para negócios jurídicos? Nesse caso eu posso tratar esses dados públicos e viabilizar esse meu modelo de negócios? Não está relacionado à finalidade pela qual esse dado é publicamente acessível?

Então, começamos a trabalhar muito mais numa lógica de ver qual é a finalidade pela qual eu publicizo o dado. E aí se quebra totalmente a dinâmica e o conceito do direito à privacidade. Pouco importa se o dado é público ou privado, o que importa é a finalidade pela qual aquele dado foi processado e está sendo publicizado. Isso vai gerar uma mudança na nossa cultura jurídico-legal brasileira. E isso está pedagogicamente colocado com todas as letras na Lei Geral de Proteção de Dados Pessoais.

Isso significa que no que diz respeito ao dado pessoal sempre se deve levar em consideração essa ideia da finalidade? Sim, mas a lei também procura trazer flexibilidade para se encontrar novas finalidades, mesmo que não sejam compatíveis com aquele contexto pelo qual o dado foi inicialmente coletado, processado e tratado. Começamos a falar, então, das bases legais.

2.5. Bases legais para o tratamento de dados pessoais: consentimento e legítimo interesse

O artigo 7º da Lei Geral de Proteção de Dados Pessoais

traz um cardápio de opções para tratar dados pessoais. São dez hipóteses, dez opções. Antes da LGPD havia somente o bom e velho consentimento. Tudo era consentimento. Era preciso autorização do titular do dado para abrir uma ficha de crédito dele, para pegar o dado dele e abrir sua ficha de controle pessoal dentro de uma organização. Tudo era consentimento, autorização do próprio titular. A Lei Geral de Proteção de Dados Pessoais elege o consentimento apenas como uma das dez hipóteses para legitimar o tratamento de dados pessoais. Isso, mais uma vez, traz flexibilidade para as organizações tratarem dados pessoais e para calçarem as suas atividades, por assim dizer.

Dentre as opções do artigo 7º está, por exemplo, a pesquisa por órgãos como o IBGE e outros da administração federal, estadual ou municipal.

A LGPD deixou claro que em determinadas situações é possível tratar dados pessoais para fins de pesquisa, por um órgão que seja conceituado como tal, e sem fins lucrativos. Pode ser para fins econômicos, mas não pode ter fins lucrativos.

E aí a lei vai expandir mesmo para política pública, para proteção à vida, execução de contratos, crédito, tutela da saúde, e assim por diante. A lei procura calibrar situações nas quais, muito além do consentimento, se conseguiria ter um fluxo de informações apropriado.

A principal inovação da LGPD foi a base legal do legítimo interesse. Legítimo interesse é um conceito que está em voga, mas o que eu queria apontar aqui é que nem sempre é fácil utilizar essa base legal porque a lei criou um ônus. Você tem o bônus de utilizar o legítimo interesse, mas você tem o ônus de demonstrar a legitimidade do seu interesse.

Por exemplo, uma rede de farmácias pede o CPF de clientes para um programa de fidelidade que concede descontos, e assim consegue formar uma grande base de dados. A seguir, pensa em usar essa base de dados para tornar suas atividades mais eficientes, pesquisando os remédios com maior ou menor saída em cada loja.

Então, aquela base de dados inicialmente estruturada para um programa de fidelidade, para dar desconto, vai ser utilizada para uma finalidade diferente da inicial. Será preciso pedir o consentimento de todos os titulares? Não necessariamente, dependendo do legítimo interesse. É preciso justificar, dizer qual é essa legitimidade do interesse, inclusive balancear com as legítimas expectativas do titular do dado. Por exemplo, o cliente espera encontrar na farmácia o remédio que vai comprar. Talvez esse seja o uso legítimo do dado pessoal para oferecer ao cliente um serviço mais eficiente.

Portanto, a LGPD oferece dez hipóteses para legitimar as atividades de tratamento de dados pessoais. Consentimento é apenas uma delas e não é a base legal mais importante, mas está no mesmo nível hierárquico das demais.

2.6. Agentes de tratamento de dados pessoais

A Lei Geral de Proteção de Dados Pessoais procura calibrar direitos e deveres de toda essa grande cadeia de tratamento de dados pessoais de acordo com o respectivo papel dessas organizações. Para isso é preciso saber quem é o controlador, ou seja, aquela entidade que determina como os dados vão ser tratados.

Se essa organização tem mais poder, ela deve ser mais responsável por toda a atividade de tratamento de dados pessoais. Ela vai ser solidariamente responsável, caso ela terceirize uma parte da sua atividade de tratamento de dados pessoais e esse terceiro viole direitos ou mesmo a Lei Geral de Proteção de Dados Pessoais. Esse terceiro seria a figura do operador, aquele que opera em nome do controlador.

Então, por exemplo, um Tribunal de Justiça, tem um terceiro que presta o serviço de armazenagem para ele numa *cloud*. Esse Tribunal teria que tomar extremo cuidado para saber quem é esse terceiro, quais os mecanismos de segurança da informação dele, porque se esse terceiro – que armazena os dados pessoais em nome do Tribunal – tiver algum incidente de segurança, o Tribunal será responsabilizado.

Isso vale para as suas atividades do dia a dia. Se você contratar um terceiro para viabilizar o pagamento da sua folha de funcionários, você é responsável por esse terceiro, assim como por aquele que instalou um *software* de processamento de dados no cartório. A LGPD procurou, de certa forma, ter esses elos de ligação de toda essa cadeia de tratamento de dados pessoais, e colocou mais obrigações, um peso maior sobre os ombros da-

quela entidade que tem mais poder, que controla toda a atividade de tratamento de dados pessoais. Por isso esse nome, “controlador”.

3. Tendências: o que deve acontecer com a entrada em vigor da LGPD?

A LGPD é uma caixa de ferramentas. Você tem que olhar para ela e ver como pode ter uma abordagem plúrima e ao mesmo tempo pragmática.

A lei recomenda que antes de mais nada você conheça os dados que tem. Faça um registro das suas atividades de tratamento de dados pessoais, faça um inventário como se fosse uma matrícula dos seus dados, a ficha corrida, relacionando todos os eventos mais importantes.

Depois de saber o que você tem em casa, comece a fazer relatórios das ações que precisam ser alteradas para entrar em conformidade. Por exemplo, o tratamento de dados pessoais com base no consentimento pode utilizar outra base legal. Não há uma finalidade apontada. É preciso uma ação para entrar em conformidade, fazer um relatório sobre isso.

Se você tem alguma atividade de alto risco para direitos e liberdades fundamentais, faça um relatório de impacto à proteção de dados pessoais. Não é assim que funciona no meio ambiente? No caso de um empreendimento que vai degradar o meio ambiente, o empreendedor faz um relatório de impacto ao meio ambiente. É a mesma lógica com a Lei Geral de Proteção de Dados Pessoais.

Você pensa em conceber novos produtos e novos serviços já levando em consideração privacidade e proteção de dados pessoais. Essa é a ideia do *privacy by design*, ou privacidade desde a concepção.

E depois de tudo isso, verifique se a sua entidade tem um programa de governança de dados. Esse programa de governança de dados vai ser o resultado desse inventário de dados que você tem, desse relatório que você tem, ou dessa metodologia de *privacy by design*. É muito além da mera política de privacidade que você vai ter dentro da sua organização. É muito além da política de segurança da informação.

Governança de dados é todo esse ferramental trazido pela Lei Geral de Proteção de Dados Pessoais. O que a lei procura, e acho que é isso que os órgãos reguladores também devem cobrar, é que você seja o mais responsável possível.

Difícilmente vamos ver uma organização 100% *compliant*, 100% em conformidade, assim que a lei

entrar em vigor.

Olhando para a Lei Geral de Proteção de Dados Pessoais, se você fez um relatório de impacto, se você tem um código de boa conduta, se você tem um programa de governança de dados, e se você tem algum elemento de *privacy by design*, você é mais responsável, a sua atividade traz menos risco e você é o mais colaborativo. Consequentemente, você vai ser menos reprovável. Em muitas situações, a autoridade pode discordar de você, pode entender que não é o caso de legítimo interesse. Mas você foi lá e fez um teste de legítimo interesse, você tem todos os registros das suas atividades de tratamento de dados pessoais, e a autoridade vai levar isso em consideração.

Pode ser o mesmo caso para a organização A e B, só que a organização A ativou todas essas ferramentas, procurou ser o mais responsável possível. Essas duas organizações deverão ser tratadas de maneira distinta, porque isso está no desenho da lei. É essa a ideia. Com base nisso, o que a gente espera, até a LGPD entrar em vigor, e depois disso também, é um processo de maturação de várias fases.

Provavelmente, primeiro teremos as fiscalizações da própria Autoridade Nacional de Proteção de Dados Pessoais, bem como dos Procons, defensorias, Ministério Público, e assim por diante. O segundo passo seria verificar como as organizações irão se juntar com seus pares e fazer códigos de boas condutas.

Por exemplo, será que os registradores não podem verificar quais são os seus problemas comuns e pensar em soluções comuns? Verificar, por exemplo, anonimização no setor de registro imobiliário, no setor de registro de pessoas naturais?

A LGPD abrange desde o setor de energia elétrica, passando pelo padeiro e pelo açougueiro ali na esquina e indo lá para a grande empresa de tecnologia. O que o legislador quis foi estimular boas práticas setoriais, que devem ser levadas em consideração.

No final, a gente tende a ver cada vez mais proteção de dados pessoais e privacidade como elemento reputacional. Provavelmente, consumidores e cidadãos irão fazer escolhas baseados no grau de proteção de dados pessoais que uma organização oferece. Temos o direito de portabilidade, que está previsto na LGPD, e, ao final de tudo isso, espero que tenhamos uma cultura de proteção de dados pessoais no Brasil, com profissionais cada vez mais engajados e organizações não governamentais olhando especificamente para essa pauta.

Se olharmos para a década de 1990, quando surgiu o Código de Defesa do Consumidor, estava todo mundo com medo.

Décadas depois, o CDC trouxe muito mais civilidade para o mercado de consumo, as pessoas se sentem muito mais confiantes. As organizações que entenderam essa mensagem até hoje colhem os frutos.

Eu espero que essas mesmas externalidades positivas se reflitam na Lei Geral de Proteção de Dados Pessoais.





A Lei Geral de Proteção de Dados em debate

– Proteção de Dados e os Registros Públicos



O Poder Público



FERNANDO ANTONIO TASSO

Juiz de Direito do TJSP. Graduado pela PUC-SP. Especialista em Gestão e Governança de Tecnologia da Informação pela FIAP. Coordenador de Tecnologia da Informação e Direito Digital da EPM onde também é Coordenador do Núcleo de Estudos em Direito Digital.

na LGPD – regime jurídico aplicável aos serviços notariais e de registros

Em primeiro lugar, gostaria de expressar minha satisfação em participar deste Seminário sobre a LGPD e os serviços extrajudiciais.

Minha missão consiste em tratar da Lei Geral de Proteção de Dados sob a ótica dos registradores e notários, tendo em especial consideração a necessidade de aprofundar o debate sobre aspectos que serão objeto de regulamentação pela Corregedoria Geral da Justiça.

Para tanto, vamos falar sobre as normas atinentes ao Poder Público, que se encontram, em franca maioria, no Capítulo IV da Lei, iniciando pela definição legal de Poder Público, na qual se incluem os serviços extrajudiciais. Trataremos ainda das bases legais aplicáveis ao Poder Público, dos princípios e peculiaridades aplicáveis aos registros públicos, compartilhamento de dados, breves anotações a respeito dos direitos do titular, obrigações, responsabilidades e sanções; e finalizarei elencando marcos operacionais de implementação.

Nesse último tópico, tentarei pontuar alguns aspectos que eu acho que vão nortear o caminho a ser seguido neste momento de *vacatio legis*, em que estamos entre o debate e a implementação da Lei Geral da Proteção de Dados Pessoais.

Quem é o Poder Público

A Lei Geral de Proteção de Dados Pessoais faz remissão ao artigo 1º da Lei de Acesso à Informação, já demonstrando uma complementaridade entre essas leis, um diálogo entre elas, dizendo que Poder Público é composto da administração direta, e aqui temos Executivo, Legislativo, e Judiciário, Tribunal de Contas, que é órgão do Legislativo, Ministério Público e Defensoria Pública.

Na redação original da Lei Geral de Proteção de Dados Pessoais era feita a remissão do artigo 1º da LAI, que veio antes da Emenda Constitucional 80, que tornou a Defensoria Pública uma entidade autônoma e de conformação constitucional idêntica ao Ministério Público.

Compõe também o Poder Público a administração indireta. São autarquias e fundações, empresas públicas, sociedades de economia mista. As duas últimas submetem-se ao regime de direito público, se estiverem atuando em regime de monopólio, praticando atividade típica do Poder Público. Contrariamente, se estiverem desempenhando atividade econômica em regime concorrencial, subsumem-se às normas de proteção pertinentes ao setor privado. Finalmente, a Profa. Maria Sylvia Zanella Di Pietro entende que, por possuírem personalidade jurídica atribuída por lei, os consórcios públicos também integram o Poder Público.

Os serviços extrajudiciais integram, com toda propriedade, o Poder Público para fins de tratamento da LGPD, por força do artigo 23, §§ 3º e 4º.

As duas disposições específicas se destinam a lhes atribuir um tratamento idêntico ao dispensado a todas as demais pessoas jurídicas de direito público e para estabelecer que uma das missões consiste em fornecer o acesso eletrônico aos seus dados para a administração pública, já que é parte dessa constelação.

Essa missão já é desempenhada com extrema eficiência. Temos os bons exemplos do portal da ARISP, portal da ARPEN, o SRI, que é exemplo de um projeto promissor. Tais portais eletrônicos proveem acesso a esse relevante serviço tanto ao Poder Judiciário quanto ao Ministério Público, à Defensoria Pública e outros órgãos públicos.

Bases legais de tratamento de dados pessoais pelo Poder Público

Conforme apregoa o professor Bruno Bioni, a LGPD apresenta um cardápio de dez bases legais de tratamento. Como sabemos, toda operação de tratamento de dados pessoais deverá estar atrelada a uma base legal, que a lei denomina requisito de tratamento em seu artigo 7º.

A professora Laura Schertel Mendes propõe um mo-

delo geral de aplicação da LGPD que se vê retratado neste esquema com três raias.

Quando a lei fala em tratamento de dados pessoais, a primeira questão que se coloca é: quais são as condições para que eu possa tratar dados pessoais?

Portanto, para que eu, Poder Público, possa tratar dados pessoais, devo me remeter a dois aspectos específicos da LGPD, que são os princípios de proteção de dados e as bases legais de tratamento.

As bases legais de tratamento estão previstas no artigo 7º da lei e integram um rol taxativo de dez hipóteses.

De princípio, é importante estabelecer que não existe qualquer prevalência entre elas. Nem mesmo o consentimento que é, provavelmente, a base legal mais conhecida, tem qualquer prevalência sobre as demais. A meu ver, termina sendo justamente o oposto, porquanto não tendo a operação de tratamento se encaixado em qualquer das nove outras hipóteses, o consentimento sana o problema de falta de base legal.

A LGPD tem no Regulamento Geral de Proteção de Dados Europeu (GDPR) sua inegável inspiração, porém temos em nossa norma uma base legal inédita. A proteção do crédito, prevista no inciso X do referido artigo, é o que doutrinadores chamam de uma jabuticaba, pois só existe no Brasil. Segundo o regulamento europeu, a hipótese de proteção do crédito está abarcada pelo legítimo interesse.

Tratamento de dados pessoais

Dentre as bases legais de tratamento de dados pessoais previstas no artigo 7º da lei, a única que declina expressamente seu destinatário, qual seja o Poder Público, é a do inciso III.

É pertinente observar que o artigo 7º, inciso III prevê que, para aqueles órgãos que executam políticas públicas, as hipóteses de tratamento de dados pessoais devem estar contempladas em leis ou regulamentos, ou respaldadas em contratos, convênios ou instrumentos congêneres.

Pessoalmente, entendo ser perigoso o termo “instrumentos congêneres”, porquanto seria desejável o embasamento em diplomas normativos dotados de maior solenidade.

Diz-se, então que o Poder Público possui uma base legal própria, que autoriza o tratamento de dados pessoais para a execução de políticas públicas. Igualmente, para o tratamento de dados sensíveis, também existe a base legal destinada ao Poder Público da execução de

políticas públicas.

Uma das críticas que se faz à redação da LGPD é que ela tem um tratamento relativamente confuso no que diz respeito ao Poder Público. Isso decorre da alternância atípica de poder que presenciamos nos últimos anos, em que num espaço de menos de cinco anos, três foram os Presidentes do Brasil e, conseqüentemente, a sensibilidade em relação ao tema da proteção de dados pessoais. Tal contexto resultou numa legislação suficiente, porém dependente de um esforço incomum do intérprete para agregar disposições esparsas em seu texto, fora do Capítulo IV, para o desenho do regime jurídico aplicável ao Poder Público.

Uma demonstração dessa aparente atecnia legislativa se revela na análise do artigo 7º, inciso III, que trata de execução de políticas públicas pelo Poder Público.

Os serviços extrajudiciais praticam política pública? Não. Não me parece. O Poder Judiciário pratica política pública? Também não. Então, nos falta base legal para o tratamento de dados pessoais?

Exige-se aqui o primeiro esforço interpretativo. A base legal do artigo 7º, inciso III, deve ser lido combinado com o artigo 23, que está no Capítulo IV da Lei.

Esse é o entendimento da professora Miriam Wimmer que preconiza a necessidade de fazermos uma junção entre o artigo 7º, inciso III, e o artigo 23 *caput*, que fala da execução de competências legais, que é o que faz o Judiciário, e de exercício de atribuições legais, como fazem os Serviços Extrajudiciais, o Ministério Público e a Defensoria Pública.

Poderiam perguntar se não seria uma atecnia utilizar uma norma de extensão à base legal do artigo 7º, inciso III. Entendemos que não, pois a reafirmação de que essa base legal do Poder Público é um todo coeso, mas está bipartida em dois artigos, vem confirmada pelos artigos 26 e 33, que falam tanto da execução de políticas públicas quanto do desempenho de atribuição legal. Portanto, é legítima a inferência de que se trata de elementos de um mesmo núcleo conceitual.

Tratamento de dados sensíveis

Além da possibilidade da utilização do consentimento, desde que além de livre, informado e inequívoco, seja também específico e destacado (artigo 11, inciso I), existe uma base legal específica para o Poder Público tratar dados sensíveis, sem a necessidade do consentimento, nas hipóteses que forem indispensáveis pela administração pública, para a execução de políticas públicas previstas

“Quanto ao consentimento, se fosse o tratamento de um dado pessoal, bastaria que o consentimento fosse livre, informado, inequívoco.”

em lei ou regulamentos.

Quanto ao consentimento, se fosse o tratamento de um dado pessoal, bastaria que o consentimento fosse livre, informado, inequívoco. Para um dado sensível, ele deve ser livre, informado, inequívoco, mas ele também tem que ser específico e destacado.

Sem o fornecimento do consentimento, aqui também se faz necessário o emprego do método extensivo da norma, utilizando o artigo 23 para tratar não só de políticas públicas, como também do exercício de competências e atribuições legais.

Em se tratando de dados sensíveis, a lei obriga que se dê especial publicidade à operação de tratamento, conforme prevê o artigo 11, § 2º.

É importante lembrar que dado anonimizado, perde a característica de dado pessoal. Por exemplo, dados de saúde são dados sensíveis. No entanto, o uso de uma massa de dados de saúde, desde que anonimizada, não demanda publicidade porque dado anonimizado não é dado pessoal, tampouco, sensível. Esse é um exemplo de que nem sempre a dispensa do consentimento demanda a publicização, como nesse caso.

Outras bases legais

Conforme vimos, o Poder Público é aquinhado com uma base legal destinada especificamente para a administração pública. Mas, pode se valer de outras bases legais de tratamento?

A resposta é afirmativa, a depender do tipo da operação de tratamento de dados.

Ao inserir dados em cadastro específico sob controle do CNJ, por exemplo, os serviços extrajudiciais estariam cumprindo uma obrigação legal ou regulatória, baseada no artigo 7º, inciso II da lei, assim como ao permitir a consulta de dados de suas bases por outros órgãos públicos.

Não existe, portanto, impossibilidade apriorística da utilização de outras bases legais, conforme a atividade desempenhada.

Nesse contexto, tratemos de duas bases legais que podem trazer questionamentos mais complexos.

É possível que o Poder Público utilize o consentimento como base legal de tratamento?

Nos *consideranda* do GDPR é possível se identificar uma clara demonstração de ceticismo quanto à validade do consentimento quando exigido pelo Poder Público, por se tratar de uma relação jurídica desbalanceada, caracterizada pela assimetria de poder.

O consentimento se vê emasculado num contexto como esse. Então, numa relação desbalanceada, não é livre o consentimento, cuja negativa poderia implicar, por exemplo, em não fruição de um serviço público.

Na LGPD existe previsão expressa de validade do consentimento para o uso compartilhado de dados pessoais controlados pelo Poder Público com entidades privadas.

Mas, quando não expressamente previsto, são utilizáveis pelo Poder Público as bases legais do artigo 7º, inciso I, para dados pessoais e do artigo 11, inciso II, para dados sensíveis?

A professora Miriam Wimmer preconiza que, aplicando-se o teste de proporcionalidade baseado nos princípios de proteção de dados, vislumbra-se uma hipótese em que o consentimento seria válido: quando a negativa de consentimento não for excludente da fruição de um serviço público. Por exemplo, eu posso ir ao balcão usufruir daquele serviço público, ou, se me é dada uma comodidade de usar um aplicativo, um equipamento móvel e eu concordo, consentir em que sejam coletados dados da minha geolocalização, bem como marca e modelo do aparelho celular, para uma finalidade que esteja atrelada a outra finalidade que não, necessariamente, a execução de política pública, como a análise estatística da inclusão digital de determinada região.

Então aqui se vislumbra, ao menos por hipótese, a possibilidade de uso do consentimento quando não for excludente da utilização do serviço.

E quanto ao legítimo interesse?

A Lei Geral da Proteção de Dados Pessoais não tem resposta para a possibilidade do uso do legítimo interesse pelo Poder Público. O GDPR explicitamente veda ao Poder Público o uso de legítimo interesse e o motivo consiste no fato de que o único interesse do ente público



consiste no interesse público. Aqui entendido como o interesse público primário, identificado pelo interesse do bem comum, não do interesse público secundário, aquele que se refere à própria pessoa jurídica de direito público interno.

No entanto, pode-se vislumbrar, o uso do legítimo interesse na retenção de dados, sem a necessária eliminação depois de prestado o serviço público, para eventual defesa em ação de responsabilização civil movida contra o Estado.

Princípios de proteção de dados

O segundo pressuposto para que eu possa tratar dados pessoais, consiste na observância dos princípios de proteção de dados, previstos no artigo 6º da lei.

Os princípios são regidos pelo princípio geral da boa-fé, que está previsto no *caput* do artigo 6º. São, portanto, onze os princípios que inspiram o regime de proteção de dados.

O princípio da boa-fé é princípio informativo da leitura de todos os demais, tendo sobre todos uma incidência transversal.

Eles têm observância incondicional, mesmo nos casos de exceção legal, como, por exemplo, em assuntos de segurança pública, segurança nacional, investigação criminal. Muito embora não estejam sob a incidência da LGPD, a observância da base principiológica da LGPD é mandatória, conforme expressamente consignado no artigo 4º, § 1º.

Todos os princípios devem ser observados na operação de tratamento de dados pessoais, sem exceção, diferentemente das bases legais, para cujo tratamento basta uma. A observância de cada um deles consiste em autêntico filtro de proporcionalidade a legitimar o tratamento de dados pessoais.

Tal é sua importância que, no caso de transferência internacional de dados, a aferição de equivalência entre os regimes de tratamento de dados pessoais perpassa pela observância dos princípios de tratamento.

Há princípios que assumem especial importância na atividade dos serviços extrajudiciais, quais sejam os princípios do livre acesso; da qualidade de dados; da segurança; da prevenção; da não discriminação; e da responsabilização e prestação de contas.

O princípio do livre acesso (inciso IV) garante aos titulares de dados pessoais a consulta facilitada e gratuita sobre a forma de tratamento de dados, duração, bem como sobre a integridade de seus dados pessoais.

Sua finalidade é uma concretização do fundamento da autodeterminação informativa, que inspira toda a Lei Geral de Proteção de Dados.

Mas, a gratuidade é eterna e incondicional, inclusive no que toca às certidões expedidas pelos serviços extrajudiciais? Não me parece ser.

Na verdade, isso tem que ser interpretado à luz das demais normas que regem a atividade dos serviços extrajudiciais. Normas especiais são interpretadas estritamente. Assim sendo, no que concerne aos Registros de Pessoas Naturais, permanece a regra de que a primeira certidão é gratuita, porém as demais não o são.

Em reforço a esse entendimento, vale mencionar o artigo 15.1 do GDPR que prevê a gratuidade somente da primeira via. Para outras operações de tratamento, percebe-se também no GDPR, que o critério é o da razoabilidade.

A materialização do livre acesso pode se dar no formato impresso ou eletrônico, sendo este um vetor de abordagem dos portais existentes e daqueles em desenvolvimento.

Quanto à qualidade de dados (inciso V), o que se preconiza é uma garantia aos titulares de exatidão, clareza, relevância e atualização de dados de acordo com a necessidade e para o cumprimento da finalidade e seu tratamento.

As anotações cruzadas nos registros civis, e entre estes e os registros de imóveis, portanto, são colocadas sob o holofote da nova lei, no sentido de que se trata de medida de conformidade que sejam feitas com a necessária rapidez, eficiência e precisão, independentemente de qualquer ato concreto do titular de dados.

O princípio da segurança (inciso VII) preconiza a adoção *a priori* de medidas aptas a proteger os dados pessoais sob seu controle de acessos não autorizados ou de situações danosas dos próprios dados.

Nesse princípio se fundamenta o conceito de privacidade na concepção (*privacy by design*) do *software* ou ambiente de tratamento de dados.

O artigo 47 da LGPD impõe a adoção de práticas de segurança da informação por qualquer pessoa que intervenha na cadeia de tratamento. Por exemplo, se um serviço extrajudicial contrata um serviço de nuvem, contrata um operador. Todos atores que passam a lidar de alguma maneira com esses dados devem observar regras de segurança da informação. Não basta que o serviço extrajudicial esteja em conformidade. Toda a cadeia de tratamento tem que estar também.



A ausência de segurança, por outro lado, é considerada pela lei como um tratamento irregular. E, sob a ótica do Código de Defesa do Consumidor, também é um serviço eivado de vício.

A adoção de práticas de segurança da informação são um indicativo idôneo sobre a gravidade do incidente (artigo 48, § 3º). Então suponhamos: se um serviço extrajudicial adota todas as medidas de segurança da informação, e ainda assim um incidente ocorre, isso é levado em consideração na eventual penalização e em como ela é feita. Isso também é uma reprodução de toda a lógica da responsabilidade civil do regime europeu.

Significa que a segurança deve ser proporcional ao risco do tratamento. Então, por exemplo, não adianta adotar o mesmo nível médio de segurança da informação para dados pessoais e dados sensíveis. Naturalmente, dados sensíveis devem estar aderentes a um critério de segurança da informação um pouco mais rigoroso e mais atento.

Com relação à prevenção de danos, mais uma vez se observa a concretização do *privacy by design*, que deve permear os três aspectos da utilização de tecnologia no negócio, desde sistemas de tecnologia da informação, as próprias práticas de negócio, e o design físico da infraestrutura da rede, como a redundância de *data centers*, a segurança perimetral por *firewall* e tudo mais. As normas da família ISO 27000 são disciplinas específicas que permeiam esse aspecto.

A par da observância de normas de segurança da informação, as boas práticas de governança também são elencadas como medidas de prevenção de observância obrigatória aos agentes de tratamento (artigo 50).

A prevenção tem por prática o mapeamento de riscos. Existe um artefato, já preconizado pelo direito europeu, que é o DPIA (*Data Protection Impact Assessment*) que, em português, foi internalizado com a denominação de Relatório de Impacto à Proteção de Dados Pessoais, o RIPDP.

A obrigatoriedade de sua elaboração, diferentemente das normas europeias, é indicada em casos específicos como no tratamento de dados sensíveis, não constituindo uma obrigação geral, nem mesmo em relação ao tratamento de dados pelo Poder Público.

A despeito do silêncio normativo, quer nos parecer que sua elaboração pelo Poder Público decorre do princípio administrativo da eficiência, cuja violação enseja a pecha de tratamento irregular de dados, bem como submete o gestor público às penas da improbi-

dade administrativa.

Um ponto a se trazer a respeito do princípio da não discriminação é a questão do nome social e a guarda de registro de operação de tratamento.

Questão relevante consiste em definir qual o grau de confidencialidade das modificações registrais da pessoa natural quando da mudança de gênero, bem como as hipóteses legais de revelação, ainda que por previsão do artigo 37 da lei devam ser mantidos os registros de todas as atividades de tratamento de dados, que nesse aspecto vem a reforçar o que já é preconizado na Lei de Registros.

Finalmente, o princípio da responsabilização e prestação de contas. Trata-se de questão que transborda a lei e permeia as Normas de Serviço da Corregedoria Geral da Justiça.

A sanha regulatória de nossa cultura jurídica indica que a regulação virá prematuramente. É oportuna a visão do colega Alves Braga, que enalteceu as vantagens de se materializar as normas já existentes antes de se produzirem novas normas no plano regulamentar.

Parece-me uma abordagem muito sensata. No entanto, em algum momento, em alguma medida, é desejável uma regulamentação, sob pena de se criar uma situação que hoje se busca banir, que é da multiplicidade de normas sobrepostas a uma mesma situação.

Tomemos como exemplo a experiência europeia, quando a Diretiva Europeia 45/96 delegou aos estados-membros a competência de legislar a respeito de proteção de dados alinhados à norma matriz, resultando em legislações díspares e de difícil uniformização no tratamento de situações concretas. Verificada a heterogeneidade do tratamento do tema optou-se por adotar um Regulamento Geral único, de modo a preservar a fluidez e previsibilidade das relações comerciais dentro da Europa e entre seus países membros e entes externos à comunidade europeia.

Não por outro motivo que, no Brasil, existe uma Proposta de Emenda Constitucional, a de nº 17/2019, que busca não só incluir a proteção de dados como um direito fundamental no artigo 5º, inciso XII, ao lado das garantias da vida privada, intimidade e sigilo. Mas também atribuir a competência legislativa privativa da União, em seu inciso XXX.

Compartilhamento de dados e o Poder Público

O compartilhamento de dados diz respeito às condições de legitimidade para o tratamento de dados pessoais.

O assunto assume relevo no contexto em que é do conhecimento de todos que há empresas que fazem a consulta de grande massa de dados para finalidades distintas que simplesmente manter os registros públicos, seja nos serviços extrajudiciais como nos judiciais.

Conforme já sublinhado, é impossível um regramento vir a proibir o tratamento de dados. O que se busca, no conceito moderno de proteção de dados, nos dizeres de Helen Nissenbaum, é garantir um fluxo apropriado de informações pessoais. Quer dizer, não é impedir que ele ocorra, mas impor um fluxo adequado.

Suas premissas são de que seja um tratamento transparente, justificado, ou seja, baseado no consentimento ou outra base legal, e que ele seja responsável e, portanto, aderente a normas de segurança e de prevenção.

Ao tratar do uso compartilhado de dados, a LGPD utilizou uma confusa técnica legislativa ao dispor sobre o tema nos artigos 25 a 28.

O artigo 25 não apresenta dificuldades interpretativas.

Em primeiro lugar declara que os dados precisam estar em formato interoperável. São conhecidos no poder público pelo menos dois tipos de modelos de interoperabilidade, o e-PING, que é o padrão de interoperabilidade do Governo Federal, e o MNI, que é o Modelo Nacional de Interoperabilidade para o Poder Judiciário.

Preconiza ainda que os dados devem estar em formato estruturado, ou seja, em tabelas numeradas e em bancos de dados relacionais. Vinculam-se a esse tema as normas da Corregedoria Geral da Justiça, que dispõem sobre uma especificação, como a qualidade da digitalização e como deve ser armazenada.

O artigo 25 também prevê que o compartilhamento de dados pessoais deve visar uma finalidade específica, dentre as quatro elencadas. A prestação de serviços públicos é a finalidade que justifica o uso compartilhado de dados, que abrange os serviços extrajudiciais.

Para a compreensão e exegese dos artigos seguintes é necessário voltarmos à definição de uso compartilhado de dados pessoais, que está no artigo 5º, inciso XVI da LGPD.

Uso compartilhado é gênero composto por tratamento de dados de cinco espécies, que foram pinçadas do conceito maior de tratamento de dados do inciso X do mesmo artigo.

Todavia, não existe uma definição legal na Lei ou em outra norma para efeitos de aplicação da LGPD do que seria cada uma dessas atividades.

Na busca de uma clara identificação das espécies de uso compartilhado, o glossário da SERPRO, que é uma

empresa pública federal, mostrou-se a melhor ferramenta. Pelo documento, é possível encontramos uma definição para comunicação, difusão e transferência internacional. Interconexão e tratamento compartilhado são termos que não integram o glossário e, confesso, tenho dificuldades em diferenciar interconexão de outras operações que integram o conceito de uso compartilhado.

Esse entrave terminológico traz uma dificuldade real em diferenciar situações de modo a dar aplicabilidade ao confuso regime jurídico do compartilhamento de dados dos artigos subsequentes.

Isso porque o artigo 26 trata de uso compartilhado de dados entre entes públicos, sendo essa a situação em que há dois ou mais entes públicos e uma única base sendo tratada por todos.

A regra prevê que nessa hipótese, deve se atender a uma finalidade específica; que ele esteja inserido no contexto da execução de política pública ou atribuição legal, e que, finalmente, todos os princípios de proteção de dados sejam observados.

No entanto, ao tratar do uso compartilhado de dados pessoais entre um ente público e um ente privado pecou, a meu ver, em duas questões.

No mesmo artigo 26 em cujo *caput* tratou do uso compartilhado entre entes públicos, no § 1º tratou de apenas uma espécie de uso compartilhado e entre entes público e privado.

Dentre as cinco atividades de uso compartilhado de dados, o legislador destacou uma: transferência de dados, dizendo que é vedado.

A primeira das exceções é no caso de execução descentralizada de atividade pública, prevista no inciso I. Por exemplo, em caso de concessão da execução de atividade pública de construção de rodovia em que os imóveis lindeiros terão os dados de seus proprietários abertos ao concessionário para a finalidade específica de interagir em eventual expropriação.

A par da outra exceção, que consiste na transferência de dados acessíveis publicamente, o inciso IV autoriza a transferência de dados pessoais bastando que esteja previsto em lei, contrato, convênio ou instrumento congênere.

Bastaria estar previsto em lei, contrato ou convênio para que esteja justificada essa transferência? Obviamente não.

A única interpretação que parece possível é que esse inciso prevê não uma hipótese, mas um requisito que, a rigor, permeia toda atividade administrativa que atua

“O direito mais fundamental do titular do dado consiste na declaração legal de sua titularidade, conforme prevê o art. 17, sendo impossível sua desvinculação da pessoa natural.”

somente *secundum legem*.

É cediço que, diferentemente das demais hipóteses, como a prevenção de fraudes e irregularidades e o resguardo da integridade e segurança do titular, tem-se ali um requisito aditivo às demais hipóteses.

De remate, receio que a hipótese legal de resguardar a integridade e segurança dos titulares, consiste numa situação de amplitude indesejada.

Agora de volta ao conceito genérico do uso compartilhado de dados, o artigo 27 traça novas determinações. Parece-nos que, dado o tratamento de uma das situações específicas (transferência) no artigo 26, § 1º, este último artigo trata das quatro situações remanescentes que integram o gênero uso compartilhado de dados.

A regra para tais situações é a da imprescindibilidade do consentimento, mas também prevê exceções.

A primeira delas é quando o consentimento é desnecessário, ainda que desnecessário, de fato, seria dizer o óbvio.

A segunda exceção incorre, salvo engano, na mesma atecnia do inciso IV do artigo 26, porquanto dar publicidade é um requisito, relembre-se, essencial, e não uma hipótese que tudo legitima. Interpretação em outro sentido implicaria admitir que praticar uso compartilhado de dados, à exceção de transferência, entre ente público e privado seria viável, bastando aos envolvidos dar publicidade ao fato.

As exceções do artigo 26, § 1º também excepcionam a necessidade de consentimento nessas hipóteses. Ao fazê-lo, importou a apontada atecnia do outro artigo, sem ressalvas.

Também trata de uso compartilhado o artigo 11, § 3º, fora do Capítulo IV, ao prescrever que se o uso compartilhado de dados sensíveis tiver objetivo de vantagem econômica poderá ser objeto de vedação ou regulamentação pela autoridade nacional. Quer me parecer que aqui se está a tratar de um poder-dever.

Direitos do titular

Voltamos ao modelo da professora Laura Schertel Mendes para identificar que ao cuidarmos dos direitos do

titular, estamos na segunda raia, a que cuida dos procedimentos para o tratamento lícito de dados, respondendo à pergunta de como se deve tratá-los.

O direito mais fundamental do titular do dado consiste na própria declaração legal de sua titularidade, conforme prevê o artigo 17, sendo impossível sua desvinculação da pessoa natural.

Tal é a atribuição de um *status* especial a esse direito que a PEC 17/2019 busca elevá-lo ao patamar de garantia fundamental, como já se faz em outros países.

O artigo 18 trata da forma e do tempo de exercício dos direitos que a seguir, em seus incisos, serão elencados. A qualquer momento e mediante requisição denotam que se trata de uma potestade a qual o controlador não pode ignorar.

Não poder ignorar não significa não poder negar. A negativa de atendimento, desde que devidamente fundamentada no dispositivo legal que a embasa, é perfeitamente possível, sob pena de se estar tratando de um direito absoluto. Não o é a possibilidade de ignorar, ainda que ilegítima ou despropositada.

Os direitos do titular elencados no artigo 18 são eminentemente autoexplicativos, de modo que trataremos com mais vagar apenas de alguns deles.

Ao tratar do direito ao bloqueio de seus dados pessoais, a LGPD se inspirou no GDPR cujo correspondente é o direito de limitação do tratamento. A limitação é apenas temporal ou qualitativa, porquanto uma vez trazido à conformidade, o tratamento readquire sua aptidão.

Conceito análogo é o da eliminação, que consiste no apagamento definitivo. No contexto dos registros públicos, esse direito parece ceder, como regra inafastável, ao direito maior de preservação dos eventos registraes que permeiam a vida civil, especialmente em questões de mudança de gênero e filiação adotiva.

Em contexto diverso, contudo, seria demonstrável em juízo a eliminação através de registros (logs) mantidos pelo controlador.

O direito de petição, que não está elencado nos incisos do artigo 18, mas encontra-se disperso pelos seus parágrafos, é de crucial importância para identificar que a

garantia dos direitos é de sistema multiportas.

O titular de dados pode peticionar diretamente ou por representante ao agente de tratamento, seja ele o controlador (registrador ou notário) ou o operador (prestador de serviço de tratamento de dados).

Tem cabimento o direito de petição, inclusive se a base legal for diversa do consentimento. Ou seja, ainda que o tratamento de dados se dê com base legal do artigo 7º, inciso III, é cabível ao titular dos dados pedir garantia de seus direitos.

Ainda, os agentes de tratamento devem comunicar da petição de direitos os demais com quem compartilhou. Por exemplo, o serviço extrajudicial contrata o serviço de nuvem, arquivamento, digitalização, e há um questionamento pelo titular. Não basta que o registrador responda afiançando a garantia do direito. Antes, deve comunicar toda a cadeia de tratamento para que tenha ciência desse pedido e confirme a salvaguarda do direito.

Além da possibilidade de exercício do direito de petição diretamente à Autoridade Nacional de Proteção de Dados, como previsto no artigo 18, § 1º, no contexto dos serviços extrajudiciais, o titular poderá fazê-lo ao juiz corregedor permanente e à Corregedoria Geral da Justiça, conforme já era previsto na Lei de Registros Públicos.

Obrigações impostas ao Poder Público

Dentre as obrigações impostas ao Poder Público e, consequentemente, aos serviços extrajudiciais está a de nomear um encarregado. Mas, diversos questionamentos surgem ao tratar desse ator. Trata-se de uma única pessoa ou é um órgão colegiado? São pessoas de dentro do serviço extrajudicial? São pessoas de fora, contratadas? A alteração da lei pela MP 869, posteriormente convertida em lei, amplia a possibilidade que antes era a de ser uma única pessoa natural. Portanto, um ponto a se enfrentar nos serviços extrajudiciais consiste em definir qual a forma e composição desse importante interlocutor no sistema de proteção de dados.

A elaboração de um relatório de impacto à proteção de dados pessoais (RIPDP), conquanto não seja uma obrigatoriedade, parece-nos que, por comungar com o princípio administrativo da eficiência e, por que não, da moralidade, consiste num artefato obrigatório ao ente público. Portanto, ao dizer a lei que “poderá”, parece dizer “deverá”.

A observância dos padrões de segurança da informação vem como obrigatoriedade estampada no artigo 46 da Lei, assim como o registro de atividades a demonstrar

o comprometimento do controlador para com os deveres de cuidado no tratamento de dados, no artigo 37.

Privacidade na concepção (artigo 46, § 2º) e como regra (*privacy by default*) encerram o eixo obrigacional primordial dos entes públicos.

A Autoridade Nacional de Proteção de Dados

A ANPD possui três funções que se destacam nesse contexto obrigacional.

Ela poderá solicitar a realização de operação de tratamento de dados, enviar informe indicando medidas cabíveis para fazer cessar violação de dados, bem como poderá solicitar a publicação do relatório de impacto.

Cabe aqui relembrar que conquanto o regime jurídico de tratamento de dados pelo Poder Público pareça mais brando que o destinado aos entes privados, por utilizar termos como “poderá” e “solicitar”, as sanções não são menos rigorosas.

Sanções a que a administração pública se submete

A temática de sanções administrativas e regras da responsabilidade civil ocupam a última raia do modelo de aplicação da LGPD, abordando a questão das consequências do descumprimento das normas de proteção.

Pode parecer que ao ente público é destinado um tratamento mais brando que ao setor privado, porque não há previsão de multa aplicável ao setor público.

Porém, subsistem as penas de advertência com indicação de prazo para adoção de medidas e de publicização da infração, esta última, conhecida por pena infamante.

Ainda que aos serviços extrajudiciais não seja aplicável a multa sancionatória prevista na LGPD, subsiste o sistema de responsabilidade civil e administrativa prevista na Lei de Registros.

Por outro lado, eventual advertência ou publicização de eventual infração proveniente da Autoridade Nacional seria fator a ser considerado em atividade correcional permanente atribuída ao juiz de direito.

O bloqueio dos dados pessoais parece ser a pior das sanções porque implica na suspensão das atividades até sua regularização.

A sanção de eliminação dos dados pessoais que se referem à infração, por seu turno, têm lugar quando inobservado o princípio da necessidade, ou seja, são coletados mais dados que os necessários para o desempenho da atividade. Embora seja aplicável ao Poder Público, não parece encontrar contexto nos serviços extrajudiciais,

que consiste numa atividade essencialmente regulada por lei própria e que consiste justamente na guarda de dados previstos na mesma lei.

Tais sanções se aplicam sem prejuízo da Lei de Improbidade, do Estatuto do Servidor Público Federal, e da Lei de Acesso à Informação. Portanto, em se tratando de atividade administrativa, a violação de norma de proteção tem alto grau de impacto em princípios administrativos, ensejando a aplicabilidade da Lei de Improbidade, que prevê sanções pessoais ao gestor público.

No tocante à responsabilidade civil de notários e registradores, regulada pelo artigo 22 e seguintes da Lei 8.935/94, a LGPD traz questionamentos acerca do diálogo entre os sistemas uma vez que o artigo 42, § 1º, inciso II, da Lei Protetiva prevê a responsabilidade solidária por ato do operador. Seria essa a hipótese de extensão da responsabilidade do delegatário ou já estaria abrangida no atual sistema de responsabilidade civil?

Por outro lado, as excludentes de responsabilidade do artigo 43 da LGPD socorreriam o registrador ou notário, ampliando as hipóteses de defesa previstas na Lei 8.935/1994?

Ou ainda, por não estarem previstas no Capítulo IV, referente ao Poder Público, as excludentes se aplicariam aos entes públicos ou a estes seria aplicado o regime próprio da responsabilidade administrativa?

A questão da obrigatoriedade da publicação do relatório de impacto, e a complementaridade ou derrogação da Lei de Acesso à Informação consistem em outras questões que desafiarão os estudiosos do tema.

Marcos operacionais na implementação da LGPD

Nesta última parte, trataremos de questões de governança e códigos de conduta, dando fechamento ao último item do modelo geral de aplicação da LGPD.

Se fôssemos concretizar todos os aspectos teóricos que tratamos em marcos operacionais a serem trilhados rumo à implementação da Lei Geral de Proteção de Dados, caberia pontuar os seguintes.

- **Conscientização interna e externa** – É justamente isso que o presente Seminário proporcionou: a conscientização e o debate construtivo. São as palestras, cursos e *workshops* que se propõem a criar uma cultura de proteção de dados, sempre atenta à questão de divisar um desafio real de um problema suposto.

- **Proposição de regramento à Corregedoria Geral da Justiça** – As entidades representativas receberam ofi-

cio da CGJ e, com espírito cooperativo devem contribuir com soluções para a regulação desse setor específico do Poder Público.

- **Oficialização de um encarregado em cada uma das serventias** – Haverá de existir aquele que vai fazer a interlocução com os órgãos de controle, promover a elaboração do relatório de impacto, proporcionar a revisão de contratos com os operadores.

- **Implementação de um programa de privacidade** – Por que estamos falando em um programa de privacidade? Porque o programa é um ciclo contínuo. A implantação da Lei Geral de Proteção de Dados em qualquer órgão ou instituição, consiste em um projeto. Ao terminar o projeto inicia-se um ciclo infindável em que se vão aprimorando as práticas de governança, tornando-se um programa em constante evolução, com observância do ciclo de vida dos dados pessoais e a incondicional salvaguarda dos direitos do titular.

Como fecho, trago essa conhecida frase do Pequeno Príncipe, propondo sua releitura: “Tu te tornas eternamente responsável por aquilo que tratas”. Tratou o dado, é responsável, eternamente.





**Princípio de
divulgação
com rogação
em xeque.**

Legitimidade
para postular
a produção
da publicidade
registral em suas
várias modalidades



A proposta que eu trouxe é uma análise



CALEB MATHEUS RIBEIRO DE MIRANDA
Oficial de Registro de Imóveis, Títulos e Documentos e
Civil das Pessoas Jurídicas de São Vicente (SP)

sobre como a LGPD modifica a publicidade nos registros públicos e modifica, de certas formas, o princípio da rogação para obtenção dessa publicidade.

Evidentemente, nós estamos fazendo uma análise antes da consolidação jurisprudencial, antes de eventual normativa da corregedoria, então, como toda análise prospectiva, certamente haverá aperfeiçoamentos a serem realizados no que for exposto, mas eu quis trazer um sistema coerente do ponto de vista interno.

Eu dividi a apresentação em quatro partes principais. Primeiramente, vamos abordar os princípios aplicáveis à publicidade dos registros públicos. Na sequência, vamos ver a questão da análise do interesse na obtenção da publicidade registral. Em seguida, os tipos de publicidades registrais, e, por fim, os critérios para verificar a legitimidade de um pedido de publicidade ao Registro de Imóveis.

1ª PARTE: PRINCÍPIOS APLICÁVEIS À PUBLICIDADE DOS REGISTROS PÚBLICOS

1.1 Princípio da Publicidade

O primeiro princípio que já foi repisado muito nas palestras é o princípio da publicidade. Eu não vou me delongar quanto a isso; o foco central é que os registros são públicos e possuem como objetivo trazer ao conhecimento do público situações que são inscritas nos livros registrais. E especialmente em relação aos Registros de Imóveis, todas as suas funções se vinculam a essa cognoscibilidade. O registro é público, e nós temos efeitos decorrentes do registro e da possibilidade de seu conhecimento. Seja quando o ato registral em si tem efeito de publicidade-notícia, seja quando possui efeitos perante terceiros, seja mesmo no registro constitutivo, a finalidade é sempre a mesma: a cognoscibilidade do assento registral.

Mais especificamente em relação à certidão, três artigos merecem atenção detida: o art. 16, § 1º, da LRP, que prevê que os oficiais são obrigados a lavrar certidão do que lhes for requerido; o art. 17 da LRP, que prevê que qualquer pessoa pode requerer certidão do registro sem informar ao oficial o motivo ou o interesse do pedido, e o art. 30 da LNR, que especialmente me chamou a atenção porque prevê que são deveres dos notários e oficiais de registro facilitar *por todos os meios* o acesso

aos dados do registro. Então a intenção dos Registradores, de acordo com o comando legal, é permitir que as pessoas conheçam os dados do registro da maneira mais eficiente para o cumprimento das suas finalidades, desde que sejam legítimas.

1.2 Princípio da conservação

O segundo princípio aplicável à publicidade dos registros públicos é o princípio da conservação. A sua previsão primeira está no texto constitucional, ao prever, no art. 236, que a atividade é exercida em modo privado, ou seja, a conservação do acervo registral é realizada pelos delegatários. A LRP também prevê, no art. 22, que para os livros saírem do cartório, deve haver autorização judicial.

Além da previsão na Constituição Federal e legislação registral, a conservação também pode ser tratada no âmbito da LGPD, porque ela é considerada uma hipótese de tratamento de dados. A LGPD inclui na definição de tratamento não só a transmissão, que é necessária para a publicidade, mas também considera tratamento o arquivamento e o armazenamento dos dados. Por isso, em relação aos dados pessoais, o registro tem o princípio da conservação, mas também se aplicam as regras da LGPD.

Tradicionalmente, nós consideramos a conservação em três aspectos:

- 1) organização racional dos registros, para que seja possível encontrar aquilo que se está buscando;
- 2) conservação no sentido de impedir a destruição parcial ou total do acervo; e
- 3) conservação no sentido de impedir alterações indevidas no conteúdo do registro.

Ao considerar as modificações ocorridas com a utilização de formas de armazenamento digitais, nós podemos verificar uma nova faceta da conservação, que seria a conservação enquanto impedimento ao acesso indiscriminado aos dados do registro.

Então, quando se fala de conteúdo registral em livros digitais, não basta que isso seja mantido no cartório somente no sentido de se ter os atos corretamente organizados em poder do Oficial, mas também impedir

a duplicação (ou cópia) do conteúdo desses livros fora do cartório. Isso também poderia ser aplicado considerando-se um acervo escriturado em meio físico, mas ganha maior relevo e importância quando consideramos o registro em meios eletrônicos.

Então nós temos três funções decorrentes dessa nova faceta da conservação:

- 1) Impedir a varredura indiscriminada de dados do registro;
- 2) Impedir a transmissão do conjunto de dados do registro como um todo; e
- 3) Impedir a duplicação do acervo registral.

Pode-se pensar numa obrigação de não só manter o registro organizado e dentro da esfera de controle do Oficial, bem como, ao mesmo tempo, conservar os registros, globalmente considerados, fora da esfera de controle de particulares que não tenham interesse legítimo no seu conteúdo, de forma a proteger os dados pessoais constantes do registro.

1.3 Princípio da publicidade proporcional

O terceiro princípio que eu busquei trazer é uma aplicação da proporcionalidade do direito administrativo ao âmbito registral. Podemos falar numa publicidade que seja proporcional.

E o que é uma publicidade proporcional? Ela pode ser vista por dois aspectos.

Primeiro, ela deve atender ao princípio da menor ingerência possível. Então, se houver várias formas de publicidade que puderem ser utilizadas para atender a uma finalidade, deve ser utilizada aquela que menos ingresse na esfera de direitos do cidadão.

Em segundo lugar, podemos falar em uma proporcionalidade em sentido estrito, no sentido de que as vantagens obtidas com aquele interesse, tendo em vista a publicidade que se pretende, devam ser superiores à restrição que se produzirá aos direitos do titular.

Portanto, os princípios são: a publicidade e a cognoscibilidade dos registros como regra; a conservação, também no sentido de impedir acesso indiscriminado aos dados do registro; e a publicidade proporcional, que exija a utilização do meio menos severo e uma ponderação para verificar se as vantagens decorrentes da publicidade superam as restrições que ela implicará.

1.4. Da escolha da forma de publicidade pelo Oficial

Existe um item nas Normas de Serviço da CGJ do Estado

de São Paulo sobre a publicidade que merece atenção específica. O item 149.1 diz:

“149.1. Cabe exclusivamente aos oficiais a escolha da melhor forma para a expedição das certidões dos documentos registrados e atos praticados no Cartório.”

Ao se fazer uma primeira leitura desse texto, parece que aqui se coloca uma questão procedimental. O Oficial escolherá a melhor forma de expedir a certidão de acordo com a conveniência dos serviços do cartório, ou seja, a forma mais adequada para se ter maior eficiência.

Mas, considerando o escopo da LGPD é possível fazer uma nova leitura: cabe aos oficiais a escolha da melhor forma, considerando como critério qual a forma que mais proteja os interesses dos titulares.

Desse modo, entendemos que, quando o Oficial pode escolher entre várias formas de publicidade ele deve optar por utilizar aquela que atenda à finalidade legítima do solicitante, mas ao mesmo tempo, a forma de publicidade escolhida deve resguardar ao máximo os interesses dos titulares dos dados.

2ª PARTE: ANÁLISE DO INTERESSE NA OBTENÇÃO DA PUBLICIDADE

2.1. Comprovação do interesse para obter publicidade registral

Vistos esses princípios iniciais, passamos à análise do interesse para a obtenção das informações registrais. Como o regime jurídico da LGPD já foi tratado extensamente no seminário, eu não vou me deter nisso – aplicam-se principalmente os princípios da finalidade, da necessidade, da adequação, da segurança e da prevenção.

Eu gostaria de trazer o aspecto de serem, os dados do Registro de Imóveis, dados de acesso público com previsão específica no art. 7º, §§ 3º e 7º, da LGPD.

Pela aplicação do princípio da finalidade, previsto na LGPD, o interesse na obtenção das informações registrais deve ser legítimo e específico (art. 6º, inc. I). Contudo, ao tratar dos dados de acesso público, a LGPD traz disposições específicas sobre o tema, e o faz trazendo dois dispositivos que parecem conflitantes.

No art. 7º, § 3º, a LGPD menciona que o acesso, ou a utilização, dos dados de acesso público para novas finalidades, deve considerar a finalidade e o interesse público que justificaram sua disponibilização; mas no § 7º do mesmo artigo, ela fala em utilização para novos fins, desde que sejam legítimos e específicos.

Dessa forma, o que parece aqui é que a lei não quer

“Se alguém quiser uma certidão do indicador pessoal, deve justificar o motivo. E também, para os demais casos de certidão, a lei não dispensa a exigência de comprovação do interesse.”

que os fins sejam só legítimos e específicos (o que já era previsto no art. 6º, inc. I, e é reforçado no art. 7º, § 7º), mas também se exige que os fins pretendidos sejam compatíveis com os fins que levaram ao ingresso dos dados no registro (art. 7º, § 3º). Por isso, é essencial identificar qual a principal finalidade do Registro de Imóveis, e podemos identificá-la como a promoção de alterações jurídicas com efeitos reais (sejam direitos reais ou outros direitos com efeitos reais), com autenticidade, segurança e publicidade (art. 1º da LRP).

De modo mais abrangente, e considerando também a razão econômica para o surgimento dos Registros de Imóveis, podemos indicar que os novos fins para os quais se pretenda utilizar os dados dos Registros de Imóveis têm que ser compatíveis com o objetivo de aperfeiçoamento jurídico e econômico do sistema de constituição, modificação e publicização dos direitos reais imobiliários.

Ao se indicar a necessidade de avaliar o interesse na obtenção de uma certidão, é preciso esclarecer de início que a LRP tem um artigo que prevê uma exceção, e que muitas vezes é interpretado como sendo a regra. O art. 17 da LRP indica que, para se obter “certidão do registro” não é necessário indicar o interesse ou motivo do pedido ao oficial. Contudo, isso não quer dizer que para nenhuma certidão seria exigida comprovação do interesse, mas só para aquelas que puderem ser consideradas “certidão do registro”. E isso envolve somente as certidões de atos registrais. E os atos registrais são a matrícula (art. 167, *caput*, da LRP), o registro, a averbação (art. 167, incisos I e II, e art. 172, *caput*, todos da LRP), a inscrição e a transcrição (art. 168, da LRP). Para a certidão desses atos, é desnecessária indicação do interesse. Consideramos, ainda, que a certidão com base no indicador real também se enquadra nessa situação, pois seu objetivo é somente identificar a matrícula relativa a certo imóvel (art. 179 da LRP).

Quanto a outras certidões, como a certidão do indicador pessoal, parece que não podemos considerá-la certidão “do registro” para fins de dispensa da comprovação do interesse por parte do solicitante. E isso porque

seu objetivo não é encontrar certos imóveis dos quais se deseja certidão, mas fazer um inventário da situação patrimonial de certa pessoa, no aspecto dos direitos reais imobiliários, e, em consequência desse inventário, solicitar eventualmente as certidões. O indicador não é um livro de prática de atos registrais propriamente dito, mas de indexação das informações constantes de outros livros. No caso do indicador pessoal, um indexador de informações sobre o patrimônio de cada pessoa cujo nome conste dos registros.

Embora pareçam semelhantes as certidões do indicador real e do indicador pessoal, distingue-se que na certidão do indicador real o indicador é somente um meio de se identificar os registros, enquanto na certidão do indicador pessoal a indexação é o próprio objeto da certidão.

Suponhamos que, por curiosidade, alguém queira saber quais imóveis uma pessoa tem no Brasil inteiro. Haveria legitimidade para essa pesquisa? Parece-me que, por mera curiosidade, não. Então, se alguém quiser uma certidão do indicador pessoal, deve justificar o motivo. E também, para os demais casos de certidão, a lei não dispensa a exigência de comprovação do interesse.

Então, nós temos que o interesse na obtenção da publicidade registral:

1) Não precisará ser indicado – e consequentemente, tampouco precisará ser comprovado – nos casos de certidões do registro, ou seja, certidões de matrículas, transcrições ou inscrições e certidões feitas com base no indicador real; e

2) Nos demais casos, o interesse deverá ser indicado e comprovado, e deve atender a três critérios: legitimidade, especificidade e compatibilidade com os fins dos Registros de Imóveis.

2.2. Análise casuística do interesse

Eu quis trazer uma série de finalidades pretendidas para verificação se os interesses indicados atendem os três critérios necessários.

A primeira finalidade é direcionamento de publicidade. Suponhamos que o solicitante indique que realizará

uma incorporação imobiliária no bairro de Higienópolis, aqui em São Paulo, e deseja saber em quais endereços residem as pessoas que compram imóveis em Higienópolis. Esse interesse parece que é legítimo, é específico e é compatível com a finalidade dos registros públicos, ao buscar mais eficiência na oferta e, em consequência, na transferência dos bens.

Quanto à curiosidade com relação aos bens de uma pessoa física particular, temos uma situação diversa. Embora seja possível a certidão de bens, e haja uma variedade de motivos para tanto (credores que buscam bens do devedor, cônjuge que deseja saber quais bens imóveis tem o outro cônjuge, análise da existência de patrimônio para aceitar garantia pessoal ou mesmo para identificar inexistência de aquisição prévia de imóveis para fins de concessão de desconto nos emolumentos, como previsto no art. 290 da LRP), não parece possível a certidão com base na mera curiosidade. Deverá ser indicado o motivo da solicitação, e o Oficial avaliará a necessidade ou não de comprovação desse interesse de acordo com as circunstâncias do caso concreto.

Quanto à curiosidade em relação ao patrimônio de pessoa pública ou de pessoa jurídica, parece que então há um interesse legítimo decorrente de se tratar de uma informação com potencial interesse público. Se não me engano, há um caso na Espanha em que já se decidiu que, no caso de pessoa pública, haveria interesse jornalístico na obtenção daquela informação, então seria possível obter a certidão com esse fundamento. E, em relação à pessoa jurídica, da mesma forma parece que o interesse é legítimo, especialmente porque a LGPD é aplicável somente aos dados pessoais das pessoas naturais (Art. 1º).

Duplicação do acervo para fins de estudo (de forma genérica): o interesse de estudo é legítimo, mas não é específico, embora o interesse de estudo em si seja compatível com o Registro de Imóveis (mas, a duplicação não).

Criação de um cadastro de devedores: até pode ser um fim legítimo e específico, mas não é compatível com o fim do Registro de Imóveis.

Criação de cadastro de conviventes, para saber que pessoas convivem em relações afetivas não matrimoniais: fim totalmente ilegítimo.

Implementação de políticas públicas. Esse é um fim legítimo? Parece legítimo que se obtenham esses dados para implementar, mas não é um fim específico. Nós vamos ver mais adiante alguns detalhes sobre Administração, mas é essencial que as requisições feitas por ela também atendam aos princípios da LGPD.

Por fim, centralização das informações dos Registros de Imóveis. Imaginemos que alguém pense que dá muito trabalho ir aos três mil Registros de Imóveis do Brasil pegar as informações. “Eu vou criar uma entidade privada, como se fosse um despachante, para centralizar, e vou obter as informações com esse terceiro intermediário.” Isso também não é possível, é incompatível com o regime de delegação essa centralização das informações registrais com o particular.

Conteúdo restante do quadro:

- Criação de índices econômicos: interesse legítimo, específico e compatível.
- Análise textual e de evolução linguística: interesse legítimo e específico, mas não compatível com finalidades do RI.
- Administração da Justiça em caso concreto: interesse legítimo, específico e compatível.
- Aperfeiçoamento das normativas registrais: interesse legítimo, específico e compatível.
- Vinculação de nomes e potencial econômico: interesse ilegítimo, específico e incompatível.
- Estudos jurídicos: interesse legítimo, mas não específico, embora compatível.
- Preservação de acervo histórico: interesse legítimo, específico e compatível.

2.3. Análise do interesse e proporcionalidade

A análise da qualificação do interesse na obtenção de certa publicidade passará, então, pela verificação em cinco etapas:

- 1) Se o pedido for de certidão de matrícula, ou com base no indicador real, não será necessário verificar o interesse, e posso ir ao passo 4. Nos demais casos, será analisado o interesse.
- 2) O interesse deve ser comprovado, e será exigido maior formalismo de acordo com o maior potencial lesivo das informações solicitadas.
- 3) Será aferido se o interesse é legítimo, se é específico, e se é compatível com os fins do Registro de Imóveis.
- 4) Feita a análise do interesse, será verificado se o pedido de publicidade atende a proporcionalidade em sentido estrito, ou seja, se as vantagens que se obtêm com a publicidade são maiores do que as restrições dela decorrentes.
- 5) Por fim, esse interesse vai direcionar a forma de publicidade que será utilizada, optando-se pelo meio que implique a menor restrição possível à proteção dos dados pessoais.

A ideia é a verificação não só do interesse necessário à obtenção da publicidade, mas também do atendimento ao princípio da publicidade proporcional. E, uma vez atendidos esses requisitos, que não seja utilizada somente uma forma de publicidade, só certidão de inteiro teor para todos os casos, mas que seja utilizada a forma mais adequada para cada situação.

3ª PARTE: PUBLICIDADES REGISTRAS

3.1. Publicidade registral quanto à integralidade ou seletividade das informações

O terceiro ponto que é importante considerarmos é a questão da publicidade. É possível classificar a publicidade registral em razão da seletividade ou integralidade das informações publicizadas.

Nós temos na lei a previsão de solicitação de informações ao Registro de Imóveis (art. 16, item 2), que aqui em São Paulo chamamos de “pedidos de busca”. Temos a previsão da certidão de inteiro teor, da certidão em resumo ou relatório (art. 19 da LRP), e ainda a previsão, nas normas paulistas, da visualização eletrônica da matrícula (item 367 e ss.).

São basicamente quatro os modelos, e eles podem ser divididos em dois grupos principais. Os grupos de publicidades que são integrais, que são a certidão de inteiro teor e a visualização de matrícula, e os grupos de publicidade que são de dados específicos do registro, que são as certidões em resumo ou relatório e as informações, nos quais se tem mais granularidade no controle da informação que será transmitida.

Além dessas quatro situações, parece que poderíamos pensar numa quinta situação, que seria uma proposta denominada “transmissão de dados”. Teríamos, nesse caso, uma transferência das informações registrares a um terceiro, mas com a assunção de obrigações específicas.

Suponhamos, por exemplo, que o usuário tenha um interesse legítimo na análise de todo o acervo registral. Se nós simplesmente transferirmos esse acervo por completo, ele acabará por ser duplicado nas mãos de um terceiro, permitindo inclusive tratamentos posteriores incompatíveis com a finalidade inicialmente alegada, e isso não vai atender a Lei de Proteção de Dados Pessoais.

Contudo, parece possível contornar essa situação. Podemos utilizar o mecanismo da LGPD para fazer a transmissão desses dados, mas com algumas restrições específicas em relação aos parâmetros em que eles serão utilizados. Podemos pensar, por exemplo, numa limi-

tação temporal ao armazenamento dos dados. Trazer a previsão de que os dados serão utilizados, mas o usuário vai se comprometer – e isso será verificado – a excluir os dados logo após o fim do tratamento. Ou por outro lado, vamos transmitir os dados, mas desde que o receptor cumpra tais requisitos de segurança. É a proposta de um novo modelo de publicidade, com relação ao qual serão abordados mais alguns aspectos na sequência.

3.2. Publicidade registral quanto à sua abrangência

A publicidade registral pode também ser classificada quanto à sua abrangência. Temos, então, a publicidade tradicional, a publicidade transversal e a publicidade global.

3.2.1. Publicidade tradicional

Primeiramente, nós temos a publicidade tradicional, que é a publicidade por certidão de matrícula ou pelos indicadores, seja indicador pessoal ou real. Essa publicidade pode se referir tanto a uma como a algumas matrículas, mas a característica específica é que se busca obter a informação integral sobre certos registros. Sobre o objeto da certidão, seja o imóvel, seja o inventário patrimonial de certa pessoa, o usuário deseja obter a informação completa.

Analisemos o seguinte modelo de um registro fictício:

Situação imóvel

R.7. Protocolo nº 56.742, em 24/08/2017. Registrado em 25/08/2017. Nos termos do Contrato particular nº 8.1234.456789-0, de 23/07/2017, **CAIO SILVA**, brasileiro, advogado, RG nº 12.345.678-9-SP, CPF nº 987.654.321-00, solteiro, residente e domiciliado à Rua nº 1, nº 234, em São Paulo/SP, **VENDEU** o imóvel desta matrícula a **TÍCIO SOUZA**, brasileiro, advogado, RG nº 23.456.789-0-SP, CPF nº 999.888.777-65, solteiro, residente e domiciliado à Rua nº 2, nº 345, em São Paulo/SP. Valor da venda: R\$100.000,00 (cem mil reais), sendo R\$50.000,00 pagos à vista e R\$50.000,00 nos termos do financiamento constante do R.8. (Assinatura do Oficial). -----

R.8. Protocolo nº 56.742, em 24/08/2017. Registrado em 25/08/2017. Pelo instrumento mencionado no R.7, **TÍCIO SOUZA ALIENOU FIDUCIARIAMENTE** o imóvel desta matrícula em favor do **BANCO FINANCIERO S/A**, CNPJ nº 00.000.000/0001-00, com sede no Setor Bancário Sul, Quadra 99, lote 9, em Brasília/DF, para garantia de dívida no valor de R\$50.000,00 (cinquenta mil reais), pagável nas seguintes condições: Prazo de 10 meses; sem juros; Parcelas no valor de R\$5.000,00. Vencimento da primeira parcela: 24/09/2017. *Valor para fins de seguro e leilão extrajudicial:* R\$95.000,00. *Prazo de carência:* 30 dias. (Assinatura do Oficial). -----

Para saber a situação do imóvel, o usual é a entrega de todas as informações que constam da matrícula ao usuário (embora isso tenda a ser modificado com a implantação do registro eletrônico, momento em que a regra será a expedição de certidão da situação atual da matrícula).

Vemos que a publicidade tradicional tem duas especificidades:

1) O objeto é delimitado em razão dos modelos tradicionais de identificação dos dados, ou seja, busca-se a informação pelo número de registro ou pelos indicadores.

2) Informações são solicitadas de forma ampla, e geralmente é utilizada a certidão de inteiro teor para se dar essa informação.

3.2.2. Publicidade transversal

Nós temos uma nova forma de publicidade que surge atualmente, ou uma nova forma de busca de dados do registro, que é a publicidade com abrangência transversal.

O que é a publicidade com abrangência transversal, ou simplesmente publicidade transversal? É aquela publicidade em que o solicitante deseja – em relação a várias matrículas do cartório ou até com relação ao conjunto total de matrículas – a obtenção de certos dados específicos para uma finalidade determinada, mas adequadamente desvinculados dos dados pessoais.

Por exemplo, se o solicitante desejar saber informações sobre quais os direitos reais de garantia mais frequentes em relação a cada imóvel, ou pessoas de quais nacionalidades são proprietárias do maior número de imóveis, é possível, no momento da expedição da certidão, fazer um corte transversal no conjunto de matrículas e obter certas informações para atender à específica finalidade para a qual se solicita. Vejamos alguns exemplos.

Exemplo 1: identificação dos endereços dos contratantes.

Domicílios

R.7, Protocolo nº 56.742, em 24/08/2017. Registrado em 25/08/2017. Nos termos do Contrato particular nº 8.1234.456789-0, de 23/07/2017, **CAIO SILVA**, brasileiro, advogado, RG nº 12.345.678-9-SP, CPF nº 987.654.321-00, solteiro, **residente e domiciliado à Rua nº 1, nº 234, em São Paulo/SP.** **VENDEU** o imóvel desta matrícula a **TÍCIO SOUZA**, brasileiro, advogado, RG nº 23.456.789-0-SP, CPF nº 999.888.777-65, solteiro, **residente e domiciliado à Rua nº 2, nº 345, em São Paulo/SP.** Valor da venda: R\$100.000,00 (cem mil reais), sendo R\$50.000,00 pagos à vista e R\$50.000,00 nos termos do financiamento constante do R.8. (Assinatura do Oficial). -----

R.8, Protocolo nº 56.742, em 24/08/2017. Registrado em 25/08/2017. Pelo instrumento mencionado no R.7, **TÍCIO SOUZA** **ALIENOU FIDUCIARIAMENTE** o imóvel desta matrícula em favor do **BANCO FINANCEIRO S/A**, CNPJ nº 00.000.000/0001-00, com sede no Setor Bancário Sul, Quadra 99, lote 9, em Brasília/DF, para garantia de dívida no valor de R\$50.000,00 (cinquenta mil reais), pagável nas seguintes condições: Prazo de 10 meses; sem juros; Parcelas no valor de R\$5.000,00. Vencimento da primeira parcela: 24/09/2017. **Valor para fins de seguro e leilão extrajudicial:** R\$95.000,00. **Prazo de carência:** 30 dias. (Assinatura do Oficial). -----

Destaque dos endereços do vendedor e comprador.

Se o usuário desejar saber as regiões nas quais moram as pessoas que mais compram imóveis, é possível fazer um corte nas matrículas para obter essas informações sem obter o conjunto total de informações. Nós teríamos uma excessividade de informações, se enviássemos todo

o conteúdo da matrícula. E mesmo o envio das informações destacadas não deve se dar exatamente como consta da matrícula. Antes da entrega devem ser depuradas de modo a permitir a identificação do endereço aproximado, mas sem indicar a numeração exata e completa. Por exemplo, poderá constar a rua e a quadra, ou a altura aproximada, mas não o número exato.

Exemplo 2: identificação das condições de aquisição e dívida.

Condições aquisição e dívida

R.7, Protocolo nº 56.742, em 24/08/2017. Registrado em 25/08/2017. Nos termos do Contrato particular nº 8.1234.456789-0, de 23/07/2017, **CAIO SILVA**, brasileiro, advogado, RG nº 12.345.678-9-SP, CPF nº 987.654.321-00, solteiro, residente e domiciliado à Rua nº 1, nº 234, em São Paulo/SP. **VENDEU** o imóvel desta matrícula a **TÍCIO SOUZA**, brasileiro, advogado, RG nº 23.456.789-0-SP, CPF nº 999.888.777-65, solteiro, residente e domiciliado à Rua nº 2, nº 345, em São Paulo/SP. Valor da venda: **R\$100.000,00 (cem mil reais)** sendo **R\$50.000,00 pagos à vista** e **R\$50.000,00 nos termos do financiamento** constante do R.8. (Assinatura do Oficial). -----

R.8, Protocolo nº 56.742, em 24/08/2017. Registrado em 25/08/2017. Pelo instrumento mencionado no R.7, **TÍCIO SOUZA** **ALIENOU FIDUCIARIAMENTE** o imóvel desta matrícula em favor do **BANCO FINANCEIRO S/A**, CNPJ nº 00.000.000/0001-00, com sede no Setor Bancário Sul, Quadra 99, lote 9, em Brasília/DF, para garantia de **dívida no valor de R\$50.000,00** (cinquenta mil reais), pagável nas seguintes condições: **Prazo de 10 meses; sem juros** Parcelas no valor de **R\$5.000,00** Vencimento da primeira parcela: **24/09/2017** **valor para fins de seguro e leilão extrajudicial:** R\$95.000,00. **Prazo de carência:** 30 dias. (Assinatura do Oficial). -----

Destaque dos elementos relevantes com relação às condições de aquisição e dívida.

Se o usuário quiser saber as condições de aquisições mais comuns, como a natureza do negócio jurídico, o preço e as condições de pagamento, qual a modalidade de garantia utilizada, o valor devido e a forma de pagamento, é possível realizar também a seleção das informações relevantes. O solicitante, demonstrado o interesse econômico em obter essas informações, não necessita de todos os dados da matrícula, e tampouco deve obtê-los à custa da proteção dos dados pessoais. Basta que o Oficial transfira esse subconjunto de dados para que a finalidade possa ser atendida.

A publicidade transversal tem as seguintes características:

1) A delimitação do objeto não é feita pelos modelos tradicionais, mas de forma ampla abrange-se todo o acervo registral ou um subconjunto dele.

2) São solicitadas informações de forma específica, mas que não abrangem dados pessoais constantes do registro, nem permitem sua vinculação.

3.2.3. Pressupostos técnicos da publicidade transversal; o surgimento da publicidade global

A publicidade transversal exige dos cartórios uma organização específica das informações. A Lei dos Regis-

tros Públicos, ao prever a certidão por quesitos, previu a possibilidade de entrega de informações selecionadas e depuradas, mas com base num modelo de processamento das informações por um ser humano. Atualmente, as certidões por quesitos são feitas de modo artesanal, com análise do conteúdo dos registros detalhadamente feita pelo Oficial ou seu substituto.

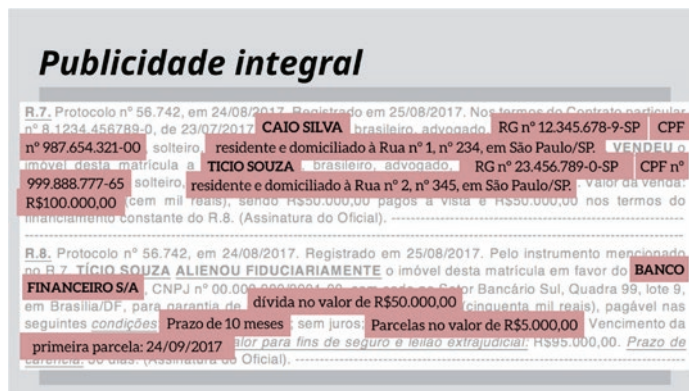
Para atender a um pedido de publicidade transversal, que pode abranger uma centena ou mesmo milhares de matrículas, a utilização do método manual implica um custo que inviabiliza o próprio serviço. Como as informações são ainda mantidas obrigatoriamente nos livros físicos, e o sistema de registro eletrônico de imóveis não foi plenamente implantado, a maioria dos cartórios não está preparada para selecionar e entregar esse conjunto de dados. Para realizar a seleção desses dados de maneira compatível com o valor atribuído ao serviço de certidão, seria necessária a existência de um sistema com base de dados bem estruturada, respeitada uma ontologia adequada, e com processos automatizados de busca e identificação da informação. Infelizmente, a maioria dos cartórios não está apta à emissão da publicidade transversal.

Surgiu uma tentativa, por parte dos usuários dos serviços, de obtenção das informações independentemente da sua estruturação interna, e que se demonstrou uma deturpação da sistemática existente. À tentativa de se obter esses dados por meio da solicitação da publicidade tradicional em quantidades massivas denominamos publicidade global.

Publicidade global é o modelo de publicidade no qual o solicitante simula um pedido de publicidade no modelo tradicional, geralmente por certidão de matrícula, mas que, pela amplitude do pedido ou da sequência de pedidos, acaba por envolver toda uma região, ou indistintamente, todo um lote de números de matrículas. O objetivo pretendido pelo solicitante é que, com a duplicação de parte do acervo, ele próprio possa fazer posteriormente a busca das informações que entender adequadas.

Quando se utiliza a publicidade global para atender a uma finalidade de publicidade transversal, são transmitidos vários elementos sensíveis, que deveriam estar disponíveis nas mãos de terceiros somente em casos que fossem necessários. O atendimento a esses pedidos acaba por criar uma duplicação do acervo registral, o que implicará necessariamente no surgimento de uma falha de segurança. Isso pode permitir que esses dados vazem e, com isso, informações sensíveis – como o nome

da pessoa, onde ela mora, o valor utilizado na aquisição do imóvel, a dívida contraída – podem ser obtidas por terceiros que tencionem utilizá-las em prejuízo dos interesses da pessoa.



informações sensíveis constantes dos registros, e que são indevidamente publicadas no modelo de publicidade global.

Sempre que se devesse utilizar uma publicidade transversal, mas é utilizada uma publicidade global, cria-se um risco maior para os dados pessoais constantes do registro.

Temos por características da publicidade global o seguinte:

1) A delimitação do objeto não é feita pelos modelos tradicionais, embora possa se utilizar deles de forma simulada (como num pedido das matrículas de número 10.000 a 10.100). O que se pretende, de fato, é a obtenção de informações de forma ampla, abrangendo todo o acervo registral ou um subconjunto dele.

2) São solicitados dados pessoais constantes do registro, seja porque o pedido é de informações integrais do registro (quando feita por meio de certidão de inteiro teor ou remessa completa de dados), seja porque, mesmo que solicitadas informações de forma específica, elas abrangem dados pessoais constantes do registro.

3.3. Combinação dos critérios: as situações de publicidade

Combinando o primeiro critério (seletividade ou integralidade das informações) com o critério da abrangência (publicidade tradicional, transversal ou global), verificamos a existência das seguintes situações principais referentes a solicitações de publicidade:

1) Publicidade tradicional integral, que abrange todo o conteúdo de um ou alguns registros. Por exemplo: certidão de matrícula, de transcrição ou de registro no Livro nº 3.

2) Publicidade tradicional seletiva, que abrange parte do conteúdo de um ou alguns registros. Por exemplo: certidão de propriedade, de ônus reais e dos indicadores.

3) Publicidade transversal, que abrange certos dados de um subconjunto de registros, mas de forma a não implicar um risco à proteção de dados pessoais, referindo-se a elementos dissociados da identificação das pessoas constantes do registro. Por exemplo: certidão indicando preço médio dos imóveis em certa região, ou frequência de transferência da propriedade ou de onerações.

4) Publicidade global integral, que abrange todo o conteúdo de um subconjunto de atos registrares. Por exemplo: todas as matrículas de uma região, ou uma sequência numérica de matrículas (lotes de matrículas).

5) Publicidade global seletiva, que também abrange, assim como a transversal, certos dados de um subconjunto de registros, mas, nesse caso, incluindo elementos que identificam as pessoas constantes do registro. Por exemplo: um pedido de certidão que abrangesse os direitos reais existentes e seus titulares.

É de notar que, quanto à publicidade transversal, ela é sempre seletiva; não podemos falar em publicidade transversal de conteúdo integral, uma vez que é característica específica desse tipo de publicidade não abranger a integralidade dos dados constantes do registro. Daí a razão de serem 5, e não 6, as situações principais decorrentes da combinação dos critérios.

Por outro lado, a distinção entre publicidade transversal e publicidade global seletiva pode parecer, a princípio, artificial, porque a publicidade transversal seria, em teoria, uma publicidade global seletiva. Contudo, a diferença entre ambas está em que na publicidade transversal não há risco à proteção de dados pessoais daqueles que constam dos registros, porque a transversalidade implica que não são abrangidos esses dados. Ou seja, não há uma identificação dos titulares, tendo a seleção de dados efeitos práticos de anonimização. Já na publicidade global seletiva a seletividade abrange dados pessoais dos titulares e por isso, como veremos, ela exigirá o cumprimento de certos requisitos específicos.

Em resumo, tanto a publicidade global como a transversal envolvem dados referentes a um subconjunto de registros. Distinguem-se, contudo, quanto à amplitude dos dados que são solicitados:

1) Se são solicitados todos os dados de um subconjunto de registros, denomina-se essa publicidade como publicidade global integral.

2) Se são solicitados certos dados de um subconjunto de registros, e esses dados identificam os titulares (dados não anonimizados), denominamos essa publicidade como publicidade global seletiva.

3) Se são solicitados certos dados de um subconjunto de registros, e esses dados não identificam os titulares (dados anonimizados), denominamos essa publicidade como publicidade transversal.

O objetivo deste trabalho é examinar quais seriam os requisitos para obter as informações correspondentes a essas solicitações de publicidade. A publicidade tradicional não nos traz desafios específicos além dos já indicados acima, referentes à análise do interesse e, em certa medida, da publicidade proporcional, pois está bem regradada na nossa Lei de Registros Públicos. O desafio que se coloca aos juristas, então, é saber como lidar adequadamente com a publicidade transversal, e como lidar com a publicidade global, tanto no aspecto de atos de inteiro teor como de dados específicos.

A intenção final do jurista é identificar a adequada aplicação do princípio da publicidade proporcional. Precisar-se-á ser verificado o atendimento à proporcionalidade em sentido estrito, no sentido de se ver se a finalidade indicada justifica a transferência dos dados, e também o atendimento ao princípio da menor ingerência possível, para identificar qual será a forma de publicidade utilizada, dentre as existentes no ordenamento.

Podemos, até então, assim resumir os requisitos para a qualificação das solicitações de publicidade:

3.3.1. Da qualificação da publicidade tradicional

Se o tipo de publicidade solicitado é tradicional e referente a certidão “do registro” (leia-se, certidão de matrícula, de transcrição ou inscrição, ou de Livro 3, ou ainda certidão com base no indicador real), a análise do Oficial é simplificada. Não será necessário analisar o interesse da parte, haja vista a dispensa pelo art. 17 da LRP, e também não precisaremos analisar a proporcionalidade, tanto em sentido estrito como no aspecto da menor ingerência possível, dado o sentido definitivo da previsão legal.

O único fator que deve ser analisado é se o pedido de publicidade tradicional não está sendo utilizado de forma simulada, quando o que realmente se pretende é a duplicação do acervo. Indicativos dessa simulação são pedidos com padrões numéricos racionais (Ex: matrículas de números 12.101, 12.111, 12.121 e 12.131) ou sequenciais, no caso de aberturas de matrículas que não se

“Notícias de vazamento de dados não são incomuns, mas raramente se ouve falar de vazamento de dados dos cartórios, exatamente porque a organização dos dados é distribuída.”

deram em decorrência de um mesmo ato (Ex: matrículas de números 12.100 a 12.120). O problema é que essa solicitação pode ser feita por intermédio de diversas pessoas (Ex: empresa que cada dia manda 30 funcionários diferentes pedirem, cada um deles, 10 matrículas diversas, para composição de seu acervo).

Ainda no âmbito da publicidade tradicional, é possível também que seja solicitada uma certidão com relação aos bens de certa pessoa. Conforme entendemos, a certidão do indicador pessoal não se enquadra na regra do art. 17 da LRP, porque não se trata de certidão “do registro”, mas sim numa certidão com base em indicador, cujo objeto principal é a indexação. Nessa situação, a verificação da possibilidade da obtenção da informação patrimonial sobre certa pessoa exige do Oficial a análise do interesse que embasa tal pretensão, devendo-se verificar sua legitimidade, especificidade e compatibilidade com os fins dos registros públicos.

Dessa forma, quanto à publicidade tradicional, a decisão do registrador limita-se a este grau de amplitude. Se o pedido é de certidão de matrícula ou certidão do indicador real, basta verificar que não se trata de pedido simulado com o fim de se obter publicidade global. Se o pedido é de certidão do indicador pessoal, será feita a análise do interesse do solicitante, para verificar se é legítimo, específico e compatível.

3.3.2. Da qualificação da publicidade global e transversal

Nos demais casos de solicitação de publicidade será feita, primeiramente, a verificação do interesse, quanto à sua legitimidade, especificidade e compatibilidade com as finalidades dos Registros de Imóveis. Na sequência, será analisado se a forma de publicidade solicitada é a menos gravosa que atende à finalidade indicada (princípio da menor ingerência possível), e se as vantagens decorrentes da publicidade solicitada superam as restrições que ela causa (princípio da proporcionalidade em sentido estrito). E então passaremos à confrontação do pedido com os requisitos da LGPD, tema abordado no próximo item.

4ª PARTE: CRITÉRIOS PARA VERIFICAR A LEGITIMIDADE DE UM PEDIDO DE PUBLICIDADE AO REGISTRO DE IMÓVEIS

Nesta última parte, o que se pretende é realizar uma análise, ainda numa perspectiva teórica, de certas situações que se apresentam aos Registros de Imóveis, e de como deve ser aferida a legitimidade, frente à LGPD, para a obtenção de certas informações que constem do registro público. Em suma, qual é a sequência de verificações que cabe aos registradores de imóveis para decidir se podem ou não fornecer aquelas informações, dar a publicidade daquele conteúdo.

A partir do momento em que falamos sobre a aplicação da LGPD, nós estamos falando de dados que não estão anonimizados. Se os dados estiverem corretamente anonimizados, nós não teremos a aplicação da LGPD, então será suficiente que seja comprovado o interesse compatível, legítimo e específico; que seja demonstrado que aquela forma de publicidade solicitada é a menos gravosa para atender ao interesse pretendido, bem como que as vantagens decorrentes superam as restrições necessárias, para que se possa dar a publicidade. Tudo isso considerando que os dados estejam anonimizados.

Se os dados não estiverem anonimizados, a verificação deve ser mais específica. Após a adequada análise do interesse e da proporcionalidade serão feitas as ponderações que se seguem.

Primeiro se verificará se a forma de publicidade solicitada atende os princípios da LGPD, especialmente os seguintes:

- 1) Princípio da necessidade ou minimização dos dados, o que implica que só podem ser transferidos os dados essenciais ao atendimento da finalidade (art. 6º, inc. III).
- 2) Princípio da segurança, que exige a utilização de medidas técnicas e administrativas aptas a proteger os dados (art. 6º, inc. VII).
- 3) Princípio da prevenção, que determina a adoção de medidas para minimizar a possibilidade de ocorrência de danos em virtude do tratamento de dados pessoais (art. 6º, inc. VII).

Concluindo-se que o pedido apresentado atende a esses requisitos será possível concluir que a forma de publicidade solicitada traz em si uma proteção suficiente para os dados dos titulares. A situação que se verificará com a transferência das informações estará de acordo com uma proteção adequada dos dados dos titulares.

Contudo, se o atendimento ao quanto requerido não responder completamente aos princípios em certo aspecto e, em consequência, resultar numa situação de insuficiente proteção dos dados pessoais, existe ainda uma última possibilidade de se permitir a publicidade: considerar a viabilidade de, se incluídas obrigações adicionais a serem assumidas pelo solicitante, com essa assunção se compatibilizaria a transferência daqueles dados com a Lei de Proteção de Dados.

Já havendo indicado a qualificação a ser realizada quanto à publicidade nas situações de publicidade tradicional, a análise da compatibilidade com a LGPD será realizada, então, frente às três situações que ainda permanecem: a publicidade transversal, a publicidade global integral e a publicidade global seletiva. Devemos ainda distinguir as situações de publicidade global, especialmente na publicidade global integral, solicitada por um particular ou pelo Poder Público, em razão da diversidade de fundamentos à decisão de cada caso.

Cabe-nos, então, a análise das seguintes solicitações de publicidade, que agrupamos da maneira mais lógica e adequada ao caso:

- 1) publicidade global integral a um particular;
- 2) publicidade global integral ao Poder Público;
- 3) publicidade global seletiva; e
- 4) publicidade transversal.

Vejamos cada uma das situações.

4.1. Da qualificação da publicidade global integral solicitada por um particular

Situação que se verifica recentemente é a recepção pelo Oficial de pedido de certidão de lotes ou conjuntos de matrículas, seja identificada explicitamente como publicidade global, seja simulada como publicidade tradicional, ou seja ainda com a indicação de uma finalidade de publicidade transversal. Nesse caso, a solicitação de acesso ao conteúdo de lotes de matrículas deve ser denegada, porque isso infringiria o princípio da conservação, retirando o controle dos registros do registrador – que é a figura constitucionalmente responsável pela conservação – e acaba por permitir um acesso indiscriminado às informações do registro. Também deverá ser negado

porque implicaria uma excessividade dos dados em relação à finalidade, infringindo os princípios da necessidade / minimização dos dados. E, evidentemente, essa centralização das informações também afeta os princípios da segurança e da prevenção.

Para ver se seria possível compatibilizar tal pedido com o princípio da necessidade poderíamos tentar imaginar uma situação em que o particular tivesse um interesse efetivo na obtenção de todos os dados do registro imobiliário. Em nosso sistema jurídico, parece não existir tal circunstância, porque efetivamente a única atividade que exige a obtenção de todos os dados dos Registros de Imóveis é a atividade registral imobiliária. Todas as outras finalidades legítimas exigiriam uma parcela dos dados, e a entrega de todos os dados evidentemente implicaria uma excessividade.

Contudo, essa situação é diversa em outros sistemas jurídicos, como é o caso do sistema norte-americano, por exemplo. Em razão de naquele país não ter se desenvolvido um sistema de registro imobiliário com uma estrutura de registro de direitos de forma oficial na maioria dos Estados, as companhias seguradoras (Title Companies) obtêm, para suas atividades, uma cópia completa de todos os atos registrados, com base nos quais elaboram uma base de dados organizada dos direitos existentes, denominadas *title plants*. E isso é legítimo no modelo norte-americano, porque embora exista um registro de títulos, a atividade de qualificação e organização jurídica das informações registrais, embora relevantíssima para o mercado, não é exercida de modo oficial, cabendo, portanto, às seguradoras, em sua atuação privada.

É necessário ressaltar que o modelo americano é essencialmente diferente do nosso. Nesse sistema, baseado em um registro de títulos em que a qualificação é feita de modo privado, a duplicação do conteúdo registral nas companhias é uma medida necessária para que se possa obter uma informação qualificada a um custo adequado, porque a organização das informações registrais é feita efetivamente junto às companhias. A duplicação do acervo para sua organização jurídica é legítima, porque supre uma necessidade do mercado imobiliário por informações confiáveis, e que não é atendida pelo Estado. Contudo, no Brasil, a realização de uma medida equivalente não configura o atendimento a uma legítima expectativa do mercado, mas é uma afronta à determinação constitucional de preservação e organização dos registros por delegatários da função registral.

4.2. Da qualificação da publicidade global integral solicitada pelo Poder Público

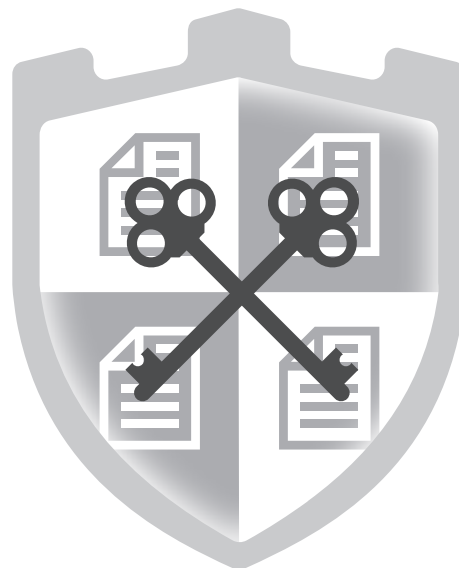
Surge então uma nova questão: se o particular não pode afrontar o comando constitucional de organização e conservação do acervo pelo registrador, porque a ele cabe a delegação dessa atividade por disposição expressa constitucional, pode o Poder Público intervir diretamente, e duplicar o acervo registral junto a seus arquivos para a realização das suas próprias finalidades?

Os três princípios da LGPD referidos quando da análise da publicidade global solicitada pelo particular também são afetados nesse caso (princípios da necessidade, da segurança e prevenção). Contudo, quando da solicitação de dados pelo Poder Público é comum que também se verifique uma afronta ao princípio da finalidade. Vejamos as especificidades.

O princípio da finalidade exige que o objetivo a ser alcançado com o tratamento dos dados seja específico. Não obstante, o Poder Público tem uma tendência a, em certos atos normativos ou administrativos, indicar expressões com vagueza semântica que não se compatibilizam com a especificidade da finalidade. Objetivos de atender o “interesse público”, auxiliar na “gestão pública”, otimizar o desenvolvimento de “políticas públicas” ou facilitar o atingimento dos “objetivos da Administração Pública” são totalmente incompatíveis com a LGPD, porque todas essas são finalidades genéricas da Administração Pública. Se for possível aceitar como legítima uma solicitação de dados por parte da Administração para fins de atender ao “interesse público”, cabe perguntar em que caso um pedido da Administração não seria para atender o interesse público? Somente em casos como de desvio de finalidade ou abuso de poder. Por isso, solicitações de publicidade global baseadas em finalidades genéricas são vedadas.

Isso não quer dizer que o Poder Público tenha que explicitamente indicar a finalidade para toda e qualquer solicitação aos Registros Públicos. Até porque, ao solicitar a expedição de uma matrícula, o próprio particular não precisa indicar seu interesse, nos termos do art. 17 da LRP. Contudo, em se tratando de pedido de publicidade que inclua dados sensíveis de forma ampla – publicidade global –, para a análise da finalidade seria essencial a indicação precisa do objetivo visado pelo Poder Público.

Outra questão que se coloca é se o Poder Público precisa de todas as informações do registro para cumprir a sua função? Parece-nos que de todas as informações ele em nenhuma situação precisaria. Ele pode até precisar



de algumas, ou de uma integralidade em certas situações, mas não de todas por completo. E uma remessa “preventiva”, para uso “potencial”, acaba por infringir frontalmente o princípio da minimização dos dados, porque ocorreria um envio de informações superior ao necessário.

A única atividade na qual poderíamos pensar que o Poder Público teria necessidade de obter todos os dados dos Registros de Imóveis seria para o exercício da atividade registral imobiliária. Evidentemente, tendo em vista a previsão constitucional quanto ao seu exercício de modo privado, qualquer atuação nesse sentido seria absolutamente inconstitucional.

Por fim, cria-se um risco à segurança dos dados com a centralização dos dados junto à Administração. Notícias de vazamento de dados não são incomuns, mas raramente se ouve falar de vazamento de dados dos cartórios, exatamente porque a organização dos dados é distribuída. Quando são centralizados os dados em um órgão, por mais respeitável e por mais avançados que sejam os sistemas de segurança que ele possua, está sendo criado um ponto único de falha, ao qual, se alguém obtiver acesso indevido, poderá acessar todas as informações depositadas naquele local.

Outra situação problemática que decorre dessa situação de a Administração duplicar as bases de dados do cartório é que se cria uma forma de acesso que é excessiva à prevista na legislação. A LGPD previu a forma de acesso da administração pública aos dados do cartório como “acesso aos dados por meio eletrônico” (art. 23, § 5º). Esse acesso pode se dar por meio de pedidos de certidões ou por ofícios, mas não seria adequado realizar uma entrega de todo o acervo para potencial utilização posterior.

Por fim, como os dados registrais são de acesso público, a Administração poderia transferir esses dados que

recebesse para entidades privadas (art. 26, § 1º, inc. III), o que aumentaria ainda mais os riscos à segurança. Para fazer uma breve menção ao SINTER, que é a situação presente sobre duplicação de dados junto à Administração, eu não acho que o SINTER seja um modelo inviável, ou que ele seja totalmente contrário ou que não possa ser implementado. Eu acredito que pode ser implementado, como ele já está funcionando, mas desde que ele não faça uma duplicação total do acervo do registro, não só porque formalmente a Administração Pública não indicou especificamente sua finalidade, mas especialmente porque esses dados, uma vez duplicados, implicariam uma excessividade de dados, oposta à minimização, e um risco à segurança.

4.3. Da qualificação da publicidade global seletiva

A próxima situação a ser abordada é a qualificação do pedido de obtenção de informações amplas sobre a situação jurídico-real constante dos Registros de Imóveis, dentre as quais dados que identificam os titulares (dados não anonimizados), à qual denominamos como publicidade global seletiva.

A principal característica dessa forma de publicidade, e que a diferencia da publicidade transversal, é que considerando o pedido pelo seu conteúdo é possível a criação de um risco à proteção de dados pessoais para o seu atendimento. E a principal diferença em relação à publicidade global integral é que somente uma parcela dos dados se mostra necessária, e eu posso ter uma situação em que, malgrado exista um risco potencial, não se está diante de um excesso de dados frente à finalidade pretendida.

Um exemplo seria uma empresa que desejasse fazer uma análise de perfis profissionais para cruzar as nacionalidades, profissões, estados civis etc., com as aquisições de imóveis pelas regiões brasileiras, para identificar o perfil de consumidores e suas aquisições de imóveis. E isso com um fim legítimo, de construir imóveis que atendam as expectativas do público.

Nesse caso, teríamos uma situação em que há uma finalidade legítima, específica e compatível com os fins do Registro de Imóveis. Contudo, ela depende da análise de um conjunto muito grande de informações. E, para fins do nosso exemplo, não poderia ser levantado esse perfil sem que contivesse informações pessoais (ainda que não todas, mas com uma anonimização imperfeita), tendo como consequências que: 1) implicaria um potencial risco à proteção dos dados pessoais; 2)

geraria uma duplicação parcial do acervo, o que seria uma restrição ao princípio da conservação enquanto manutenção do acervo sob o controle do registrador; e 3) permitiria ainda o surgimento de um novo ponto de falha ao se criar mais um local no qual esses dados poderiam ser acessados.

Esses problemas, contudo, parecem possíveis de serem contornados. Se tomadas certas medidas preventivas, podem ser reduzidos os riscos à proteção dos dados pessoais de forma a que sua transferência não seja vedada pelo ordenamento.

Vemos quatro regras principais como necessárias para a redução dos riscos:

- 1) Transmissão exclusivamente dos dados que foram estritamente necessários.
- 2) Previsão de limitação temporal para a conservação desses dados nas mãos do receptor.
- 3) Assunção de obrigações específicas por parte do receptor, dentre as quais a de apagar os dados uma vez feito o tratamento.

4) Autorização da Corregedoria Geral da Justiça tanto para análise dos termos da transferência e das obrigações assumidas como para fiscalização de seu cumprimento.

Com essas limitações, mesmo ocorrendo a transmissão de um conjunto grande de dados do registro seria possível impedir uma duplicação do acervo registral que causasse prejuízo à segurança. E para esses casos me parece que não seria suficiente uma autorização somente da Corregedoria Permanente. A questão é mais ampla, porque envolve uma quantidade substancial de dados, e por isso deveria ser verificada pela Corregedoria Geral. Então, com essa autorização e cumpridos os demais requisitos, seria possível a transferência dos dados a terceiros.

4.4. Da qualificação da publicidade transversal

A última situação a ser analisada é a solicitação de publicidade transversal, em que se requer a publicidade de certos dados de um subconjunto de registros, mas tais dados não identificam os titulares, ou seja, são dados anonimizados.

Temos para essa situação dois requisitos.

O primeiro é que os dados estejam adequadamente anonimizados. A LGPD prevê que “os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços

razoáveis, puder ser revertido” (Art. 12). Por outro lado, a anonimização precisará ser feita no âmbito do registro imobiliário, ou seja, pelos Registros de Imóveis ou no âmbito das atividades registrais, das entidades registrais.

Não seria possível, por exemplo, transferir os dados para um terceiro, que assume a responsabilidade de anonimizar antes de tratar. Seria necessário fazer esse tratamento no âmbito do Registro de Imóveis para, posteriormente, transferir. E teria que ser uma anonimização irreversível considerado o custo, o tempo, e o estado da arte (art. 12, § 1º).

O segundo requisito é que sejam transferidos somente os dados estritamente necessários. Poder-se-ia perguntar porque seria esse um requisito, uma vez que inaplicável a LGPD a dados anonimizados. Contudo, nesse caso o fundamento não é diretamente a proteção dos dados pessoais, mas a necessidade de manutenção dos dados registrais sob controle do registrador em observância ao princípio da conservação. A transmissão de dados para fora do Registro de Imóveis deve obedecer à legislação registral, e a única forma específica de publicidade que dispensa o interesse é a publicidade tradicional. Para a publicidade transversal, havendo necessidade de declarar e comprovar o interesse, é essencial que os dados apresentados se vinculem ao interesse pretendido, o que por si só é suficiente para exigir que a transferência dos dados se restrinja ao essencial para o atendimento da finalidade pretendida.

5. CONCLUSÃO

Voltando ao quadro final das publicidades, nós verificamos agora seis situações principais.

Na publicidade tradicional por certidão de matrícula ou de indicador real será desnecessário verificar o interesse, nos termos do art. 17 da LRP. A única precaução do registrador é impedir a utilização simulada do pedido de publicidade tradicional para fins de se obter uma publicidade global.

Na publicidade tradicional por certidão de indicador pessoal, ou certidões de informações específicas dos registros, será feita a análise do interesse (se legítimo, específico e compatível com as finalidades do Registro de Imóveis), e poderá ser exigido pelo Oficial um grau maior ou menor de sua comprovação, de acordo com o potencial lesivo das informações.

No caso da publicidade transversal, em que se busca obter elementos dissociados dos dados pessoais – por exemplo, saber os preços dos imóveis em certa região –

os requisitos são, além da verificação do interesse nos três aspectos, a análise da essencialidade dos dados e da adequada anonimização.

No caso da duplicação de acervo pelo particular, as principais vedações a que se permita essa publicidade são: 1) o princípio da conservação, que impede a duplicação do acervo por particulares; e 2) o fato de que essa duplicação permitiria utilização indevida dos dados pelos particulares, posteriormente. Já na duplicação do acervo pelo Poder Público, somam-se a essas questões as seguintes:

- 1) A não especificidade da finalidade, que ofende o princípio da finalidade previsto na LGPD;
- 2) A existência de um meio menos gravoso de acesso às informações pelo Poder Público, vedada a duplicação.
- 3) Os princípios da prevenção e da segurança prejudicados pela criação de um ponto único de falha.

Por fim, quanto à publicidade global seletiva, entendemos ser impossível a transferência ampla de situações jurídico-reais, inclusive com dados que identifiquem as pessoas por meio de mera certidão. No entanto, parece-nos que há uma possibilidade de se realizar essa transferência de acordo com a sistemática prevista na LGPD, desde que atendidos os requisitos propostos, quais sejam: que se refiram somente aos dados essenciais; que exista uma previsão de limitação temporal para que os dados estejam no poder do receptor; que haja a assunção de obrigações específicas, dentre as quais a de apagar os dados uma vez realizado o tratamento; e a autorização e a fiscalização sejam realizadas por parte da Corregedoria Geral da Justiça.

Gostaria de terminar com uma frase do doutor Ricardo Dip. Ele diz que o registrador de imóveis é o guardião jurídico da propriedade privada. Eu acredito que o registrador é também o guardião dos dados pessoais. Os oficiais possuem uma atividade peculiar, porque nós atuamos em uma situação jurídica em que não há a outra parte presente. Quando o solicitante requer a certidão não há oportunidade para o titular dos dados se manifestar. É o registrador que deve defender o direito desse titular, o direito ao cumprimento adequado do ordenamento jurídico.

E ainda, há um papel muito importante a ser realizado pelo registrador em relação à forma como será concedido acesso aos dados do registro, ou seja, exigindo a comprovação do interesse – quando necessário – e sempre buscando atender às finalidades legítimas do modo menos gravoso para os direitos dos titulares.



Ontologia registral – sujeitos de direito e suas representações nos Registros Públicos



Eu vou tratar do tema da ontologia



IVAN JACOPETTI DO LAGO
4º Oficial de Registro de Imóveis em São Paulo (SP)
e Diretor de Relações Internacionais do IRIB

registral especificamente no aspecto da ontologia registral que diz respeito aos sujeitos de direito e às suas representações nos registros públicos.

Para quem ainda não viu nenhuma apresentação sobre esse tema e não olhou nada a respeito, parece um tema um tanto quanto esotérico. De certa maneira é mesmo, porque o que nós vamos ver aqui é algo que diz respeito a uma visão do Registro de Imóveis para o futuro, talvez para daqui a 3, 4, 5, 10 anos. Enfim, uma visão para o Registro de Imóveis em formato totalmente eletrônico, não mais no paradigma digitalizado que temos hoje.

E a ontologia registral é uma técnica ou um método de se organizar os dados que vão compor o Registro de Imóveis no futuro. O que nós vamos ver, então, é como isso se relaciona com a nova Lei de Proteção de Dados. E é claro que, não obstante, nós tenhamos aqui como perspectiva uma visão de futuro, isso vai nos trazer uma série de reflexões que são úteis para a compreensão do sistema que temos hoje.

Ontologia usada como método para organizar informações

Ontologia, de maneira geral, é uma das vertentes da metafísica, isso no campo da filosofia, que estuda os caracteres fundamentais do ser. A pergunta fundamental da ontologia do ponto de vista filosófico é: o que é isso aqui? Essa é a pergunta fundamental. Do que nós estamos falando? O que é?

Qual ser? Tratando-se da metafísica, desse ramo da filosofia, o “ser em geral”, quer dizer, a própria existência. Então a ontologia, filosoficamente, diz respeito às características essenciais de qualquer coisa que exista de maneira concreta ou ideal. Seria talvez o campo mais abstrato da filosofia. Quer dizer, são as próprias precondições da existência do que quer que seja, do que quer que exista.

Mas há também uma série de ontologias regionais. Quer dizer, além dessa ontologia mais abstrata, mais geral, que trata da existência por si mesma, nós temos também na própria filosofia ontologias regionais que tratam das características essenciais de seres que são objetos de um certo âmbito do conhecimento.

Então eu tenho características que são de tudo aquilo

que existe, mas há certos seres que estão compreendidos em certas categorias que têm certas características próprias. E se um determinado ente não tiver essas características, não está naquela categoria na qual estão enquadrados.

A ontologia desperta algumas questões que são fundamentais na filosofia e que ainda não estão solucionadas, estão em debate há 2500 anos, como, por exemplo, a questão da diferença entre essência da existência, quer dizer, qual é a diferença entre existir e ser alguma coisa. Ainda, a distinção entre características necessárias ou acidentais, quer dizer, quais características são imprescindíveis para que algo seja aquilo que é, e quais podem ou não estar presentes conforme o caso: o ser humano, para ser humano, tem que ser, ao menos potencialmente, racional, e isso é uma característica que lhe é essencial. Se ele é alto, baixo, gordo, magro, isso é uma característica acidental, não é essencial.

E também, naquilo que nos interessa mais propriamente na ontologia registral, a questão da relação entre o ente individual e a sua ideia universal.

Aqui nós temos já um problema, que não vamos entrar em detalhes porque não é o nosso objeto: como a inteligência humana funciona. Esse é um debate que já tem 2500 anos, saber se o ser humano capta as essências dos indivíduos, ou se, ao contrário, ele reconhece nos indivíduos um conceito que existe de forma mais universal, mais abrangente, e ele pensa e faz uma relação entre uma coisa e outra.

Por que isso é interessante aqui? Isso é interessante porque, na ontologia registral, como a gente vai ver, a máquina não sabe o que é alguma coisa, mas ela pode ser ensinada a saber como uma coisa se relaciona com outra. Então, sendo bem objetivo, a máquina não sabe o que é o João da Silva, mas ela pode ser ensinada que o João da Silva se enquadra em uma categoria um pouco mais genérica, que é a categoria de pessoa. E é então, com base no estabelecimento dessas relações que vai ser construída a ontologia registral.

Então há essa relação entre entes individuais com

categorias cada vez mais genéricas, que por sua vez também se enquadram em categorias cada vez mais genéricas, e isso então vai ser um mecanismo utilizado para organizar as informações.

Na ciência da informação, então, a ontologia é utilizada como método para organização de informações. É uma maneira, por assim dizer, de se estruturar um banco de dados, ou então de se estruturar as informações de forma a possibilitar buscas cada vez mais inteligentes. Como a gente vai ver, isso vai possibilitar a realização de buscas e a realização de perguntas à máquina para as quais a máquina, em princípio, não foi construída para responder já que a gente não sabia ainda que essas perguntas seriam feitas um dia.

Essa forma de estruturação da informação vai permitir que se indague à máquina uma série de questões que, a princípio, não haviam sido previstas. E como a ciência da informação estrutura essas informações? Ela utiliza alguns elementos que vão sendo cada vez mais genéricos. O primeiro – “entes individuais” – pode ser, por exemplo, o João da Silva, pode ser o imóvel X específico. Quer dizer, são entes individuais.

Acima disso há uma categoria um pouco mais genérica que é a de classes de indivíduos. O João da Silva é: homem, pessoa natural, sujeito de direitos. Quer dizer, são todas categorias que vão se relacionando umas com as outras em um aspecto vertical. E elas, então, se relacionam com certas classes de entes individuais, classes de indivíduos, se relacionam com outros entes individuais, e as classes também se relacionam com outras classes de indivíduos.

E a essas classes podem ser ligados certos atributos. Por exemplo, a pessoa natural tem como um de seus atributos ter um estado civil. Qual é? Não sei. Pode ser solteiro, casado, separado, divorciado, mas algum ela tem. A pessoa natural tem como atributo ter um certo número de documento. O número vai variar, mas é atributo de pessoa natural ter um certo número de documento. Então esses atributos são ligados a essas classes. Isso pode ser replicado em termos de Registro de Imóveis para todos os elementos que compõem o Registro de Imóveis. E a gente vai ver quais são esses vários elementos até chegar no nosso ponto aqui, que é especificamente o ponto dos sujeitos.

Os entes se relacionam entre si, as classes entre si, as classes com os indivíduos etc. Para aplicarmos essa ideia ao Registro de Imóveis é fundamental decompor o que compõe o Registro de Imóveis, quer dizer, quais são os

elementos que estão lá no Registro de Imóveis. O que se registra? O que compõe, por exemplo, a transmissão da propriedade? Eu vou ter sujeitos, vou ter um objeto, vou ter um título, vou ter certo direito resultante. Se pensarmos num direito real limitado, a coisa já muda um pouco. Se pensarmos num direito real de garantia, muda um pouco também. Quer dizer, o que compõe cada um desses vários direitos que são produzidos pelo Registro de Imóveis?

Quais são os elementos essenciais e acidentais de cada registro? Quer dizer, o que sempre está presente em um ato de registro? O que sempre está num ato de registro de transmissão? O que é acidental, ou seja, pode estar ou pode não estar? Há elementos que são essenciais, que sempre estarão presentes, ou então aquele registro que não é um registro, e elementos que são acidentais, que em alguns casos estão presentes, e em outros não.

E quais são os atributos desses vários elementos? É claro que a descoberta desses vários elementos envolve um longo estudo de tudo aquilo que nós fazemos no Registro de Imóveis. Quer dizer, exatamente o que se faz lá? Quais são os elementos que compõem tudo aquilo que o registrador faz? E como a gente vai ver, isso muitas vezes envolve uma tomada de decisão. Por quê? Porque quando a gente categoriza um certo elemento, de alguma maneira a gente pode estar tomando uma decisão num campo que às vezes não é assim tão seguro. Apenas para citar um exemplo: o registro de uma alienação fiduciária em garantia. O credor é proprietário do bem, mas é um proprietário fiduciário. Os atributos do proprietário fiduciário são tão diferentes dos atributos do proprietário em geral, que é de se indagar se aquilo pode ser categorizado mesmo como propriedade. Então, a própria construção de um sistema como esse envolve uma série de decisões, jurídicas mesmo, sobre como classificar todos esses elementos que compõem o Registro de Imóveis.

No Registro de Imóveis o objeto é o imóvel

Quais são os vários elementos que compõem, então, qualquer registro? Sujeitos. Qualquer registro tem sujeitos. Tem um alienante, um adquirente, um credor, um devedor etc. Nem sempre nós temos situações de registro no Livro 3 que podem, por exemplo, envolver um penhor. Mas de maneira geral, o objeto, no Registro de Imóveis, vai ser o imóvel.

Ainda, um título em seus vários sentidos, o título formal e o título causal. Isso em cada sistema de Registro de Imóveis vai ser encarado de maneira diferente. Eu vou

“O estabelecimento da ontologia permite que se obtenha acesso a respostas para perguntas que ainda não foram formuladas, mas que podem vir a ser.”

ter sistemas em que um título, que por si gera efeitos reais, outros sistemas que não, que dependem de um modo de aquisição. Eu vou ter sistemas em que o título é o próprio contrato; eu vou ter sistemas nos quais eu tenho uma combinação de um contrato com um negócio jurídico real. Eu tenho sistemas nos quais eu só tenho o negócio real. Isso tem que ser estudado em cada sistema de registro para se conhecer, naquele sistema específico, quais são os elementos que vão compor o Registro de Imóveis. E além disso, os direitos resultantes. Quer dizer, quais são os direitos que podem resultar dessa combinação de um ato entre sujeitos acerca de um certo objeto que é levado ao Registro.

O desenvolvimento de uma ontologia do registro, portanto, demanda a criação de uma árvore conceitual em cada um desses elementos. Há uma pessoa específica, que é pessoa natural, que por sua vez é sujeito de direitos etc. Há o lote tal, da quadra tal, que por sua vez é imóvel urbano, que por sua vez é imóvel etc. Quer dizer, eu tenho várias categorias possíveis com atributos distintos.

E como toda classificação, não há propriamente um único modo de realizá-la. Claro que há maneiras incorretas de fazer isso; mas pode haver mais de uma maneira correta. A classificação deverá ser orientada por sua utilidade. Quer dizer, eu tenho que classificar todas essas informações de maneira que a vinculação dos atributos a essas classes às quais pertencem os indivíduos seja útil para fins de buscas, pesquisas etc. E com isso eu vou desenvolver uma ontologia do registro nessa árvore de conceitos.

As decisões, muitas vezes, são difíceis: condomínio edilício é sujeito de direitos? A princípio, não. E não obstante, às vezes, aparece como adquirente de um objeto. Ou seja, eu tenho um objeto adquirindo outro objeto.

Então é um esforço tecnológico e jurídico razoavelmente complexo o desenvolvimento dessa árvore conceitual, a fim de se classificar os vários elementos que compõem o registro.

Cada ente individual, integrante de cada classe, se relaciona com um ou mais entes individuais, da sua própria classe ou de outras: os entes da classe “sujeitos”, as

partes, relacionam-se com o ente individual da classe “objeto”, o imóvel. Quer dizer, ali naquele registro específico, se ele disser respeito a um imóvel, eu vou ter um sujeito que se relaciona com um imóvel, mas também com outros sujeitos, por exemplo, a contraparte do negócio que foi celebrado.

Mas ele pode também se relacionar com outros sujeitos além do alienante. Quer dizer, se ele é casado, por exemplo, ele tem outro tipo de relação, que é categorizada de outra maneira na árvore conceitual com o seu cônjuge, que vai produzir uma série de outros atributos e uma série de outras consequências. Por outro lado, os imóveis também podem se relacionar entre si. Quer dizer, os imóveis podem estar na mesma rua, na mesma quadra, podem ser ou não confrontantes entre si.

Então, de alguma maneira, esses entes individuais “sujeitos”, e os entes individuais “objetos”, se relacionam entre si. E esse modo de se relacionar vai variar segundo a natureza de cada classe, de cada subclasse, nas quais estão inseridas esses entes individuais. Por exemplo, na classe daquilo que nós podemos chamar “direitos reais” há maneiras distintas de se relacionar objeto, sujeito etc., segundo se trate de um direito sobre a coisa própria ou um direito sobre coisa alheia.

A propriedade fiduciária é um direito sobre coisa própria ou um direito sobre coisa alheia? É uma boa pergunta. Por vezes, para que se construa essa árvore conceitual, isso abrange tomadas de decisão sobre um aspecto jurídico envolvido naquilo que é levado a registro.

Por outro lado, sujeitos se relacionam entre si, como eu já disse, e os imóveis também se relacionam entre si. E o estabelecimento da ontologia permite, então, que se obtenha acesso a respostas para perguntas que ainda não foram formuladas, mas que podem vir a ser. Então, aqui nós temos a finalidade de tudo isso: para que serve todo esse aparato? Para que, por meio da verificação dessas várias relações, eu possa encontrar respostas sem que eu tenha que novamente reconstruir tudo.

Dou um exemplo. O Banco Mundial tem, entre seus vários programas, um que é desenvolvido juntamente com a ONU, que é o programa dos chamados Objetivos

do Desenvolvimento Sustentável (“SDG Goals”). Dentro desse programa, naquilo que diz respeito ao Registro de Imóveis, o Banco Mundial tem algumas perguntas para os vários países que o integram, perguntas essas que o Brasil nunca conseguiu responder. Primeira: No país inteiro, ou na maior cidade, quantos imóveis são de propriedade de mulher? Como responder essa pergunta num sistema analógico? Procurando matrícula por matrícula. E com o detalhe de que a matrícula não tem, a rigor, a informação “mulher”. Eu vou ter que deduzir com base nos nomes.

Segunda pergunta: quantos imóveis estão registrados no país inteiro ou na maior cidade? Não é somar as matrículas, pois tem matrícula que está cancelada, tem matrícula que está encerrada, tem matrícula que foi parcelada etc. Teria que, novamente, olhar uma por uma.

E a terceira pergunta: desses imóveis, quantos são apartamentos? Teria que pegar de novo matrícula por matrícula, olhar uma por uma. Quer dizer, o estabelecimento dessas categorias permite que, no futuro, se surgirem novas perguntas, eu não tenha que pegar todas as matrículas de novo e procurar essa informação. Por quê? Porque elas já estarão organizadas levando em conta sujeitos, objetos, títulos, direitos etc.

Isso é só um exemplo. Há muitas outras possibilidades.

O registro usa representações para vincular certas pessoas a certos imóveis e a certos direitos

Vamos ver especificamente esse assunto sob a ótica dos sujeitos. A atribuição de uma titularidade no registro, evidentemente, depende do estabelecimento dos sujeitos de direitos. Quer dizer, para que eu possa ter um titular de um direito no Registro de Imóveis, seja ele qual for, eu tenho que ter um sujeito desse direito. E esses sujeitos que têm direitos registrados, eles em si são realidades que são externas aos registros. Quer dizer, os sujeitos são as pessoas, naturais ou jurídicas, que não vivem lá no registro, vivem aí mundo afora. E que aparecem no registro mediante uma representação. Quer dizer, não há como trazer o imóvel para o registro, diretamente, nem a pessoa. O que nós colocamos no registro são representações do imóvel e representações das pessoas. E nós usamos essas representações para vincular certas pessoas a certos imóveis e a certos direitos.

Como fazemos para vincular um certo registro a uma certa pessoa concreta? Ou seja, como criar essa ligação do mundo registral com o mundo real, com o mundo concreto? Isso foi mudando ao longo do tempo. Mas

é interessante pensar que em todas as épocas sempre se fez isso recorrendo a um terceiro, que no primeiro momento era a sociedade, era a coletividade, eram as pessoas que viviam numa certa localidade, conheciam de quem se tratava; e que, num segundo momento, esse terceiro passa a ser o Estado, que passa a ser o fornecedor de documentos de identificação pessoal etc.

O que havia na primeira Lei de Registro Geral de Imóveis, de 1864, como representação dos sujeitos das hipotecas? Nome, domicílio e profissão do credor; nome, domicílio e profissão do devedor. Quer dizer, o sujeito tinha um nome, morava em tal lugar, e tinha uma profissão. O funcionamento do sistema dependia de que as pessoas soubessem quem era esse sujeito com esse nome, que morava em tal lugar, que tinha essa profissão. Era um elemento de aproximação: era possível estabelecer com certeza quem era? Bem, às vezes passados 20, 30, 40, 50 anos, ninguém mais sabia quem era o sujeito, mas é o que era possível fazer naquele momento.

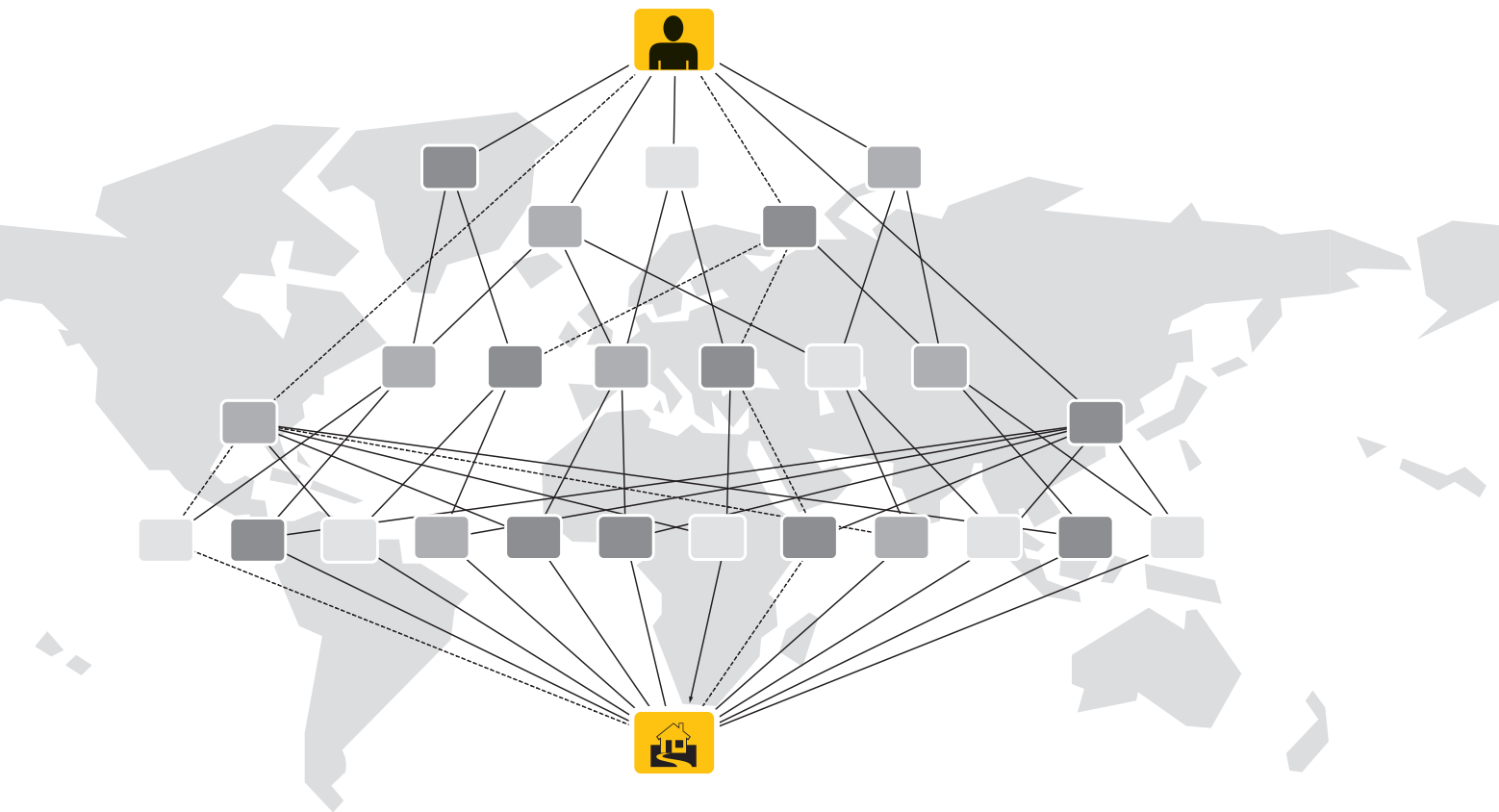
Ainda no século XIX (Decreto 370), e já no século XX, no decreto 18.542 de 1928, esses elementos são mantidos, ainda se identifica os sujeitos com nome, domicílio e profissão. O Decreto 4.857, de 1939, acrescenta mais dois elementos em se tratando de ato de transcrição, aquisição de imóvel: o estado civil, e a residência. Domicílio, residência, é até redundante, mas, de fato, esse decreto menciona os dois elementos. A rigor, o que há de inovação é a indicação do estado civil desse sujeito no registro.

A Lei 6.015 muda o paradigma, porque agora não há mais esse recurso ao conhecimento das pessoas a respeito de seus concidadãos: passa-se a recorrer ao Estado como o ente que fornece identificação das pessoas. Além de nome, domicílio, nacionalidade, estado civil e profissão, há também número de inscrição no CPF ou no Registro Geral (cédula de identidade) ou, na falta deste, a filiação.

Passamos a ter agora um número, ou mais de um número, que identifica certa pessoa. Estamos criando maneiras cada vez mais sofisticadas de representação, tornando mais difícil a homonímia, tornando mais difícil que se perca a ideia de quem era aquele sujeito com o passar do tempo.

Por que eu tenho todos esses dados no Registro de Imóveis? Tratando já de dados pessoais, por que eu tenho no registro o nome, domicílio, nacionalidade, estado civil, profissão, CPF, RG?

Claro que todos esses dados servem para aquilo que se chama “a determinação subjetiva”, ou “a especiali-



dade subjetiva”, para que eu possa com isso identificar os sujeitos. Qualquer um desses dados é útil para isso de uma maneira ou de outra. Não obstante, se pode discutir se eles não são redundantes. Existindo um CPF eu precisaria ainda desses dados todos identificando as pessoas? É que todos eles têm a função de facilitar a identificação das pessoas de alguma maneira, facilitar o cumprimento desses princípios da determinação ou especialidade subjetivas.

Representações de pessoa registral: dados que servem para identificar as pessoas e dados que repercutem na situação jurídica do bem

Com isso se estabelece a representação de certa pessoa natural. Estamos focando nas pessoas naturais por conta da ideia da proteção de dados pessoais. Podemos falar, então, que de certa maneira essas representações são uma pessoa registral. E eventualmente eu posso até ter mais de uma pessoa registral para a mesma pessoa natu-

ral, o que é uma situação patológica, mas pode acontecer.

Por outro lado, alguns desses dados vão além. Eles não se limitam a servir de subsídio de identificação das pessoas, mas repercutem na própria situação jurídica do bem. O estado civil, por exemplo, não serve somente para se identificar a pessoa. Ele serve também para que se saiba que eventualmente aquela aquisição repercuta no cônjuge. Em outros casos não repercute.

Há, então, dados que apenas servem para identificar os sujeitos, e há dados que compõem a própria definição da situação jurídica do imóvel.

E a respeito dessa identificação das pessoas, a questão das pessoas registrais. Por vezes o registrador, e também os magistrados, se veem em situações nas quais é necessário ter certeza de que aquela pessoa que está no título é a mesma que está no registro anterior. Nem sempre isso é fácil de se fazer. Veja-se o que consta desta decisão da Corregedoria Geral da Justiça do Estado de São Paulo:

“Diante disso, é necessário que a instrução seja com-

plementada mediante produção de novas provas destinadas a demonstrar que o requerente é o coproprietário do imóvel. Poderá ser feito, por exemplo, mediante solicitação de informação ao tabelião de notas que lavrou a escritura...”.

Por vezes, os elementos que estão no registro não são suficientes para se chegar na pessoa real. Por vezes a pessoa registral tem uma incompletude que faz com que não seja possível, por meio dos dados que estão ali, se chegar na pessoa específica, vai ser necessário buscar outros elementos. Em algumas situações o registrador conseguirá fazer isso ali diretamente, ele mesmo. Em outras, não. Vai ser o caso de recorrer à jurisdição por necessidade de dilação probatória etc., porque o registrador não tem possibilidade de fazer a cognição.

Esta outra decisão também é muito interessante:

“No título apresentado o nome do proprietário do imóvel partilhado consta como sendo Manoel Soares de Melo Júnior, sendo que na transcrição Nº 28751, do 16º Registro de Imóveis, o nome do titular do domínio é Manoel Soares de Melo. No título anterior, uma escritura pública datada de (16/06/1961), consta como adquirente Manoel Soares de Melo, português, casado, mas sem outros dados de qualificação que pudessem comprovar sua identidade. Além disso, da análise dos documentos apresentados, é possível constatar que o nome do pai do falecido é Manoel Soares de Melo”.

Ou seja, não há certeza quanto a quem adquiriu o imóvel. Segue:

“Entende o apelante que o óbice apresentado pelo registrador deve ser afastado na medida em que o pai do *de cujus* jamais esteve no Brasil, certo que Manoel Soares de Melo Júnior sempre se portou como proprietário do imóvel”.

Vejam, são elementos que são tão externos ao registro, que aqui, sem uma dilação probatória que o registrador não tem condições de fazer, não se vai chegar a quem é o titular. São situações que aparecem quando a pessoa registral é falha de alguma maneira.

É possível uma pluralidade de pessoas registraes relativas a uma mesma pessoa natural? Possível é, mas me parece que isso é uma situação patológica. Se eu tenho, por exemplo, uma mesma pessoa natural que aparece no registro com dois CPFs diferentes, ou com dois nomes diferentes, isso é uma situação patológica, e vai ser remediada por meio de retificação, em alguns casos diretamente pelo registrador, e em outros, inevitavelmente, se recorrendo à jurisdição por conta da necessidade de

dilação probatória etc. Mas pode acontecer. Eu posso ter no indicador pessoal, por exemplo, duas, três, quatro fichas da mesma pessoa com nomes diferentes, com números diferentes de documento etc. Pode acontecer.

Nesse caso, caberá ao registrador, ou ao juiz, encontrar qual é o elemento unificador subjacente que é a pessoa concreta, a pessoa real. A pessoa concreta é uma só, a despeito de eventualmente ela ser representada no registro por mais de uma maneira. Às vezes, no mesmo ofício de registro, às vezes, em ofícios de registro distintos. Quer dizer, ela pode aparecer com dados diferentes que vão ensejar a existência de pessoas registraes diferentes.

Portanto, há dados que servem tão somente para permitir a identificação das pessoas, para realizar a determinação subjetiva; e há alguns dados que vão além, repercutindo na própria situação jurídica do bem. Será que esses dados devem ser tratados da mesma maneira, sob o aspecto da proteção de dados pessoais, ou de maneiras distintas? Não me parece que um dado que repercute na situação jurídica do bem possa ser suprimido em termos de publicidade pelo registrador.

E os dados de determinação que são redundantes? Se há indicação do CPF, por exemplo, será que se deve continuar indicando qual é a profissão do sujeito? Ou será que esses dados são redundantes e dentro de uma ideia de minimização, que é própria da proteção de dados pessoais, a publicidade dessas informações deve ser de alguma maneira restringida? É uma questão. Será que no futuro o próprio nome não vai ser um dado redundante e só o CPF já seria suficiente para que o registro em princípio se preste? É uma provocação, evidentemente.

Outra situação: o sujeito é casado por separação absoluta de bens, então não há repercussão na situação jurídica do bem em relação ao seu cônjuge. Ele deveria ser qualificado constando os dados do seu cônjuge, que não tem qualquer relação com o bem em questão? Será que não bastaria dizer: “Fulano, casado, com separação absoluta de bens”, sem qualificação do cônjuge? São questões para levar em conta dentro dessa ideia de minimização. Quais dados se deve continuar fornecendo de maneira ampla e restrita, e quais dados não?

Sob a ótica da ontologia, especificamente, nós teríamos entes individuais: fulano de tal, é o João da Silva, o Antônio etc.; classes de indivíduos: sujeitos de direitos, pessoa, pessoa natural etc.; atributos da classe de indivíduos: pessoa natural, pode ou deve ter, então, nome, domicílio, nacionalidade, profissão, inscrição no CPF,

“Por meio de triangulações entre classes, entre entes individuais, entre atributos, nós vamos formando um conjunto de dados organizados a respeito do sujeito de direito.”

número de RG etc.; relações que se estabelecem entre indivíduos: fulano de tal é casado com ciclana de tal etc.; relações que se estabelecem entre classes e atributos: pessoas naturais brasileiras têm RG, pessoas naturais estrangeiras tem RNE.

Por meio desses vários cruzamentos, ou mais tecnicamente, dessas triangulações que são feitas entre classes, entre entes individuais, entre atributos, nós vamos então formando todo esse conjunto de dados organizados a respeito do sujeito de direito.

Ontologia registral prepara o sistema registral para fornecer informações relacionais

Para concluir, vamos tratar do acesso à informação e à proteção de dados pessoais. O sistema brasileiro de registro foi evoluindo com relação à maneira de se prestar informações. Num primeiro momento temos informações “chapadas”, ou seja, a prestação da informação ao público como mera imagem do assento que consta do livro. Por exemplo, o traslado de uma escritura manuscrita, lavrada em 1970, que não é uma transcrição digitada da escritura, mas uma cópia da escritura tal como ela está no livro. Isso é informação chapada, mera imagem do assento que consta no livro. De certa maneira, é a forma mais rudimentar de prestar essas informações, uma simples imagem do que está no livro, a interpretação do que está escrito cabe a quem receber essa certidão.

Há uma segunda possibilidade um pouco mais sofisticada, a transcrição das informações. Num segundo momento eu posso ter a digitação com base em informações que constam dos livros. Alguma interpretação eu tenho aqui, não estou entregando uma imagem do que está no livro, eu estou lendo e redigitando.

Uma terceira maneira seria a prestação de informações por quesitos, a busca no assento de um conteúdo específico. Por exemplo, se eu fornecer uma certidão que diz respeito a quem é o proprietário atual e quais são os ônus que não estão cancelados acerca de certo imóvel, eu já tenho algo um pouco mais sofisticado. Há no registro uma série de informações que não interessam ao requerente; o que interessa para ele nesse momento

é saber quem é o proprietário e se há hipoteca ou não, se há penhora ou não.

Há uma quarta possibilidade, e aqui já entramos na ideia da ontologia, que é a prestação de informações relacionais, em que eu não tenho só uma situação consolidada de certo registro, mas a possibilidade de prestar informações que são produzidas com base não só no conteúdo de um assento específico, mas na maneira como vários registros se relacionam entre si, ou como vários elementos que compõem os registros se relacionam entre si. Ao fazer constar na informação “quantas mulheres têm imóveis”, estamos entrando nessas informações relacionais, estamos tratando de um elemento específico que está em muitos registros e que, no entanto, vai gerar uma única informação. Isso seria a informação relacional.

E a ontologia registral aparece, então, como um método de se preparar o sistema registral para fornecer esse tipo de informação. Quantos imóveis foram alienados num certo bairro no dia tal? Ou então, no mês tal, ou na rua tal? Há perguntas que podem ser feitas e ainda não foram, e que poderão ser respondidas se as informações forem estruturadas dessa maneira.

Tecnologia repercute na publicidade permitindo a realização de correlações nunca antes possíveis

E quanto à publicidade?

A publicidade é um princípio fundamental dos direitos reais, e é um princípio do próprio direito privado. Na perspectiva econômica, a publicidade do registro imobiliário, especificamente, consiste no fornecimento de informações sobre a relação entre sujeito, objeto e direito relevantes para transações a seu respeito.

A tecnologia repercute muito na publicidade porque, por um lado, ela permite a realização de correlações nunca antes possíveis. (Com o uso da tecnologia podemos encontrar correlações que nem imaginávamos que existiam. Muitas vezes, as pessoas nem sabem o que elas querem encontrar na massa de dados, elas vão olhar os dados primeiro para depois saber o que tinha ali para ser descoberto). Por outro lado, o acesso a esses dados

passa a ser feito para certos acervos que antes estavam ocultos. Não ocultos em teoria, mas ocultos na prática.

E aqui surge um conceito muito interessante, que eu não acho que seja aplicável no Brasil, mas que já foi desenvolvido nos Estados Unidos e houve um caso na Suprema Corte que levou em conta a ideia de obscuridade prática, *practical obscurity*. A informação estava disponível em bancos de dados públicos, mas somente para quem soubesse onde procurar.

Trata-se de um caso de 1989, da Suprema Corte dos Estados Unidos, Departamento de Justiça *versus* a entidade “Repórteres pela Liberdade de Imprensa”. Quatro pessoas foram implicadas num certo caso de suspeita de corrupção em relação a um congressista norte-americano. E aí um grupo de jornalistas foi procurar informações sobre aquilo que seria a ficha corrida desses quatro. Nessa época havia informações criminais espalhadas nos Estados Unidos nos vários *countys*, no escritório dos vários xerifes etc. E isso era público, acessível. Quem quisesse ir lá e pedir a informação, ela estava disponível. No entanto, o FBI tinha uma compilação dessas informações para seus próprios fins de investigação. O que os repórteres fizeram? Foram no FBI, e com base na lei de liberdade de informação, pediram: “Nós queremos a compilação sobre essas pessoas”. O FBI respondeu: “Não, porque isso aqui não está aqui para divulgação pública, mas para o nosso próprio uso. O que está disponível é ir em cada xerife dos Estados Unidos e procurar as informações”.

Isso foi levado para o judiciário, e a Suprema Corte decidiu que, de fato, o FBI não tem que fornecer essas informações. Por quê? Porque se as informações espalhadas são públicas, a compilação não é. Segundo a Suprema Corte, a proteção da privacidade dessas pessoas gerava para eles um interesse na manutenção dessa “obscuridade prática” em que as informações estão espalhadas e não concentradas.

Isso é criticado pela doutrina mais recente. Um artigo de 2007 argumenta que isso foi feito em época anterior à internet, de maneira que a doutrina espera que em outro caso a Corte mude de opinião e passe a entender que essas compilações são sim acessíveis.

A publicidade tem que ser conjugada com o princípio da especialidade, ou especificidade, como se diz em alguns sistemas europeus. Isso significa, então, que a publicidade vai tornar pública a existência de um direito cujos aspectos são delimitados pela especialidade nas suas vertentes objetiva e subjetiva, bem como do direito em questão. Por isso é tão importante para nós

a questão da pessoa registral e os dados que compõem a determinação e vão permitir chegar nessas informações. Mas isso vai nos trazer o problema da proteção dos dados dessas pessoas registraes e sua repercussão nas pessoas naturais.

Exatamente por isso nós vamos ter no registro, então, uma grande massa de dados pessoais, porque a própria definição da situação jurídica dos imóveis depende da identificação desses sujeitos.

Não vou entrar aqui naquilo que já foi falado, acerca da definição de dado pessoal – dado pessoal é aquele dado que diz respeito a certa pessoa, ou que pelo contexto pode levar a certa pessoa, caso em que não se trataria de pessoa “identificada”, mas sim de pessoa “identificável”. Me parece que é um problema enorme saber exatamente qual é o limite desse identificável. Quer dizer, eu tenho a informação de uma pessoa que vendeu um imóvel num certo edifício num certo dia. Isso torna possível identificar a pessoa ou não? É uma questão para ser debatida.

Outra questão é que na União Europeia a pessoa falecida não goza, em princípio, de proteção de seus dados pessoais. Cada país-membro pode outorgar a proteção dos dados da pessoa falecida, mas, em princípio, isso não compõe o Direito Comunitário. No Brasil é uma boa pergunta, se nós temos essa proteção ou não para os dados das pessoas falecidas, se eles estão ou não protegidos para as pessoas falecidas. Os mortos têm também direito a essa proteção de dados pessoais?

Crítérios de acesso aos dados registraes

Para concluir, eu vou passar rapidamente pelo tema dos critérios de acesso aos dados registraes que existem no direito comparado.

No direito comparado há sistemas com ampla liberdade de acesso às informações, que podem ser requeridas sem necessidade de justificação. Por outro lado, há outros sistemas que exigem algum tipo de interesse justificado.

E a pergunta de um milhão de dólares é: a nova lei de proteção de dados criou algum condicionamento para fornecimento das informações para nós, registradores brasileiros?

Na verdade, pelos estudos que fiz, eu acho que não há nenhum país tão liberal no sentido de fornecimento de informações constantes do registro quanto o que temos tradicionalmente no Brasil. Mesmo nos países que não exigem qualquer tipo de justificativa isso é condicionado,

por exemplo, pelo fato de a informação dizer respeito a registro específico, ou então a dados aos quais se possa chegar por meio de um índice.

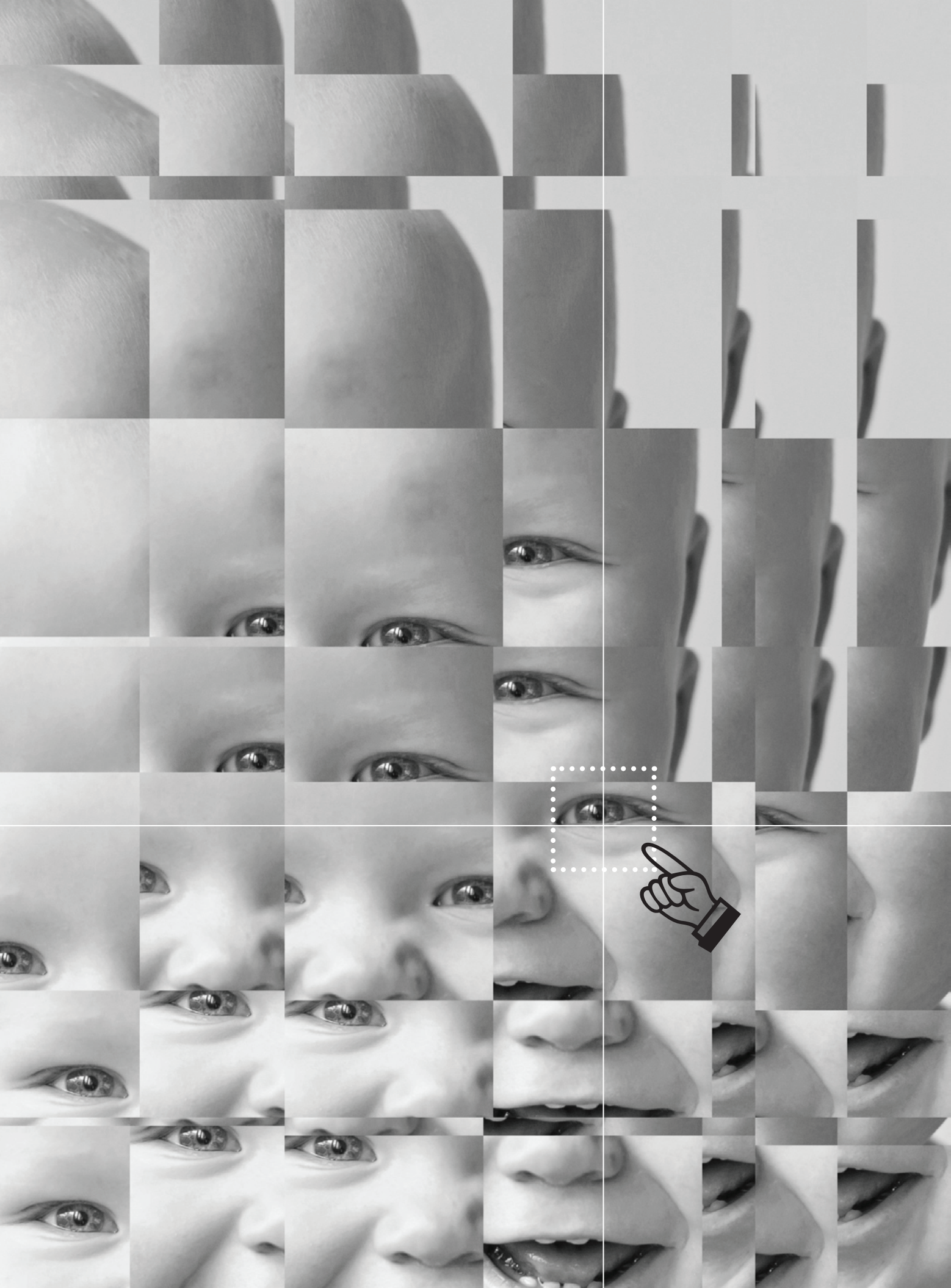
Por exemplo, não há precedente no sentido de uma pessoa solicitar informações de cédulas de crédito registradas no ano de 1988, emitidas em favor do Banco do Brasil, e que tenham um certo valor mínimo. Essa é uma informação que não está nos índices e não diz respeito a um registro específico, e que abrange assentos que dizem respeito a uma infinidade de pessoas que não se confundem com o solicitante. Um pedido dessa natureza poderia ser atendido após a vigência da nova lei de proteção de dados pessoais?

Alguns países, como é o caso da Holanda, tratam de maneira diferenciada o fornecimento de informações individuais a pessoas específicas, e o fornecimento das chamadas *bulk disclosures*, informações em lote, informações em massa. E nesses casos não é que essas informações não sejam fornecidas, elas são, mas há algum condicionante. Por exemplo, um compromisso da pessoa que está recebendo de que não vai divulgar, não vai fazer uso que ultrapasse a finalidade para a qual os dados foram entregues ao registro etc.

E finalmente, para concluir, é interessante observar o caso da Alemanha, que é um país bastante restritivo, no qual não se fornece informação sem interesse legítimo. Há toda uma jurisprudência a respeito do que é ou não interesse legítimo.

Diferentemente do que acontece na Espanha, em que também se exige o interesse, mas basta que a parte o manifeste, não cabendo ao registrador qualificar esse interesse, na Alemanha o interesse é qualificado quando do pedido. E há, então, uma série de precedentes acerca de quais interesses são ou não legítimos, quais pessoas gozam de presunção de interesse (como, por exemplo, os notários) etc. Um exemplo é a questão do *timing*. Se alguém solicita a informação com uma necessidade que virá a surgir dali a um ano, considera-se que nesse caso não há interesse legítimo. Deve o solicitante aguardar a sua necessidade chegar para então pedir a informação.





Ontologia registral – sujeitos de direito e suas representações nos Registros Públicos



Minha área de estudo e pesquisa é



MARCELO SALAROLI

Oficial de Registro Civil de Pessoas Naturais em Jacaréi (SP)

principalmente o Registro Civil das Pessoas Naturais.

Para esta palestra dei passos avançando sobre o tema da Lei Geral de Proteção de Dados, é esse conhecimento que pretendo compartilhar com vocês.

Não temos conclusões definitivas sobre o tema, mas temos conclusões, talvez provisórias, e já podemos apontar alguns caminhos a seguir. Vou aproveitar a oportunidade também para contar como é a realidade do Registro Civil, como vemos isso que estamos estudando, enfim, compartilhar nossa experiência.

Representações da pessoa natural no Registro Civil

O meu foco, então, é a pessoa natural. Ou, sendo mais específico, as representações da pessoa natural no respectivo Registro Civil. Geralmente se diz que o Registro Civil das Pessoas Naturais é o cartório que registra nascimento, casamento e óbito. Eu quero dar uma dimensão mais completa, mais abrangente e ao mesmo tempo profunda antes de entrarmos propriamente na proteção de dados pessoais, e lembrar o conceito de estado civil, que também não é apenas a informação de que tal pessoa está casada ou não, se é viúva, divorciada ou solteira. É mais que isso. É a qualificação jurídica da pessoa, resultante das diferentes posições que ocupa na sociedade, hábeis a produzir diferentes consequências. É a posição jurídica da pessoa no meio social, é esse um dos conceitos que se extrai da doutrina. Em vez de estado civil, prefiro a expressão estado da pessoa natural.

São três as dimensões do estado da pessoa natural: o estado político, o estado familiar e o estado individual. Começamos pelo estado político da pessoa natural, que se compõe da cidadania, naturalidade e nacionalidade. É o registro de nascimento, que confere cidadania às pessoas, é o reconhecimento do Estado de que existe um ser humano, o reconhecimento oficial que dá existência jurídica ou sujeito de direitos e deveres e lhe assegura o nome. A certidão de nascimento é o primeiro documento da pessoa, faz parte da documentação básica do ser humano a que todos têm direito, sendo assegurado acesso universal e gratuito por se tratar de documento fundamental para o exercício da cidadania.

É esse mesmo registro que vai dizer a naturalidade da pessoa, ou seja, a vinculação da pessoa a uma unidade da Federação, especificamente o Município, que, por regra, era o município do local do nascimento. No entanto, com uma alteração recente da lei, no momento do registro o declarante pode optar pelo local de domicílio da mãe como sendo o município de naturalidade. Essa alteração acolhe aquelas famílias que se deslocam somente para ter o nascimento em outra cidade, mas o vínculo afetivo, o município onde a criança vai morar e crescer é o domicílio da mãe por ocasião do nascimento. A lei permite, então, se atribuir a naturalidade a esse município, o que constará do registro de nascimento.

A nacionalidade tem suas regras definidas pela Constituição Federal, no artigo 12, mas elas estão todas refletidas no Registro Civil das Pessoas Naturais. Por exemplo, o critério do *Jus Solis*, pelo qual a pessoa que nasce no território nacional é brasileira. Sabemos que a pessoa nasceu no território nacional porque há um registro de nascimento. Há uma norma estabelecendo que todo nascimento ocorrido no território nacional será levado a registro.

Se a pessoa nasce no território nacional, mas os genitores são estrangeiros que aqui estão a serviço de seu país, então ela não tem a nacionalidade brasileira, porque a Constituição assim prevê. O registrador civil, então, quando registra uma pessoa nessas condições, usa outro livro, outro procedimento, que é registrar esse nascimento no Livro E, constando a observação de que aquela pessoa não tem nacionalidade brasileira. A perda da nacionalidade brasileira é um ato que entra no Registro Civil das Pessoas Naturais, porque o registro é dinâmico e deve se manter atualizado.

E a outra dimensão é o estado familiar da pessoa natural. A relação de parentesco, a filiação, adoção, negatória de paternidade. Acho que por aqui já podemos ver que o Registro Civil está sempre lidando com dados pessoais, nunca vamos estar fora do conceito de dado pessoal. Toda a nossa base está no dado pessoal. E dado pessoal

sigiloso, muitas vezes. Nós estamos acostumados a garantir o sigilo, a privacidade das pessoas.

Eu fui registrador imobiliário e migrei para as atividades do Registro Civil das Pessoas Naturais. Isso foi uma experiência bem interessante, viver com duas dinâmicas de registros públicos bem diferentes. E hoje, quando se debate aqui a certidão do registro imobiliário ser estruturada, com informações pinçadas pelo registrador, lembro que o Registro Civil das Pessoas Naturais já faz isso há muito tempo. Nós temos que pinçar do registro o que pode e o que não pode ir para a certidão. É uma matéria que rende interessantes debates dentro do Registro Civil, pois a legislação não traz muita clareza sobre o que pode e o que não pode ser publicizado. Agora, com a Lei Geral de Proteção de Dados, esse debate se renova. Por um lado, torna a questão ainda mais complexa, mas também traz um marco legislativo que poderá assegurar a atuação do registrador. Ou seja, aquelas informações que omitimos, teremos mais respaldo para omitir.

Voltando ao estado familiar no qual se insere a situação conjugal, a informação se a pessoa é solteira, casada, divorciada ou viúva. Inclusive já temos no Registro Civil das Pessoas Naturais a união estável, ainda que em caráter facultativo, é uma informação que tem publicidade no Registro Civil.

Embora a doutrina diga que união estável não altera o estado civil, evidentemente é uma posição social da pessoa com repercussões jurídicas, ou seja, tem impacto no estado da pessoa natural. Inicialmente um provimento da Corregedoria Geral da Justiça do Estado de São Paulo, atualmente um provimento da Corregedoria Nacional de Justiça, estabelece que a união estável tem a sua publicidade no Registro Civil das Pessoas Naturais.

Enfim, a dimensão individual do estado da pessoa natural. A idade da pessoa você vai saber a partir da data de nascimento que consta no registro de nascimento. O sexo da pessoa é outra informação individual que consta no registro de nascimento; eventual alteração de sexo é feita perante o Registro Civil. A capacidade civil da pessoa natural tem publicidade no Registro Civil, basta lembrar dos institutos da emancipação e curatela. A curatela, de certa forma, altera a capacidade civil, e a emancipação a antecipa. Por último, o fim da pessoa natural, seu óbito, ou mesmo a morte presumida, a ausência.

Concentração de informações sobre a pessoa e a proteção de dados

É no Registro Civil das Pessoas Naturais que todas essas

informações estão organizadas de forma sistemática para revelar a situação jurídica da pessoa nesses aspectos. Estamos tratando aqui hoje de ontologia registral, sujeitos de direito, e eu estou trazendo para vocês os aspectos da pessoa que estão representados nos registros públicos. E parece interessante esse recorte para a proteção de dados da pessoa, porque as pessoas são proprietárias de imóveis, são pais, são cônjuges, são devedores. Às vezes, são vários papéis sociais, são várias representações que se encontram nos registros públicos.

A pergunta é se poderíamos criar uma base única com todas essas informações. Ou seja, reunir num mesmo sistema não apenas as informações relativas ao estado da pessoa natural (Registro Civil), mas também as informações relativas a bens imóveis (Registro de Imóveis), dívidas (Tabelionato de Protesto), escrituras públicas e a amplidão de atos que podem abarcar (Tabelionato de Notas) e os mais diversos atos e contratos, sobre bens móveis ou mesmo bens imateriais (Registro de Títulos e Documentos), participações em pessoas jurídicas (Registro Civil das Pessoas Jurídicas). Já se cogitou, no Poder Público, formar uma superbase concentrando todas as informações referentes a uma mesma pessoa, tão abrangente a ponto de se fornecer ao sistema uma única informação da pessoa, o seu CPF, e se receber de volta todos aqueles dados, todas aquelas informações da pessoa.

Se olharmos pela ótica da proteção de dados, isso não parece nem um pouco seguro, nem um pouco interessante aos direitos subjetivos concentrar todas essas informações, todos esses múltiplos aspectos da pessoa num único sistema.

Tratamento de dados deve ser feito de acordo com a finalidade para a qual ele foi disponibilizado

Ainda na parte registral, resgato a finalidade do registro, porque o princípio da finalidade, na LGPD, é um princípio muito importante. O tratamento de dados deve ser feito de acordo com a finalidade para a qual ele foi disponibilizado. Extinta essa finalidade, deve-se extinguir o tratamento dos dados, ressalvadas exceções.

No Registro Civil das Pessoas Naturais, um efeito muito importante é constituir o meio de prova. O Código Civil é expresso ao dispor que a filiação se prova pela certidão do registro de nascimento (art. 1.603), bem como que ninguém pode vindicar estado contrário ao que resulta do registro de nascimento (art. 1.604). Podemos dizer que os atos e fatos sujeitos a registros são

“Temos essa amplitude da LGPD, que não diz respeito apenas à privacidade, mas é contra o processamento indevido para a garantia da igualdade, liberdade, democracia.”

provados por meio do próprio registro. É de grande utilidade para a sociedade e comunidade jurídica ter um documento com fé pública para comprovar determinados atos e fatos. Ainda que não se elimine completamente os questionamentos e impugnações, pelo menos se reduz enormemente, bem como se restringem os meios pelos quais isso poderá ser questionado.

Outra finalidade dos serviços notariais e de registro é garantir a publicidade, autenticidade, segurança e eficácia dos atos jurídicos, de acordo com o artigo primeiro da Lei dos Notários e Registradores, a Lei 8.935/1994.

Podemos dizer, assim, que os registros públicos buscam proteger as relações jurídicas da pessoa, seja na relação com o estado, seja na relação com as outras pessoas. Quando se fala em registros públicos muito se fala de “dar segurança jurídica”, expressão que o público leigo às vezes não entende muito bem, pois segurança jurídica é um conceito abstrato. Mas quando um carro é roubado, o dono quer a segurança de que sua posição de proprietário será respeitada, para que não seja tão simples aos criminosos transferir a propriedade. Ele quer segurança jurídica. Se alguém tem um imóvel ou vários outros direitos registrados no registro público, essa pessoa quer segurança jurídica, quer proteção. Quer ser conhecido como proprietário, como titular dos direitos, que é a segurança jurídica estática.

O mesmo ocorre na visão dinâmica. Para transacionar bens e direitos vamos buscar informação jurídica segura para poder firmar um bom contrato, então vamos ao registro público, que é a fonte atualizada de informações seguras e confiáveis. Essa é outra característica muito interessante do Registro, que é ser o repositório onde deságuam todos os títulos referentes àquele bem ou àquele pessoa, todas as alterações. Então tem que estar tudo lá e organizado. Há um recorte muito sistemático, já antigo e ainda muito útil, uma tecnologia antiga dos registros públicos feitos no papel, mas com muita eficiência, por isso perdura até hoje, porque tem utilidade para as pessoas.

Eu não acredito que seja possível extinguir esse serviço prestado dessa forma. É até possível mudar quem

presta esse serviço, mudar o jeito que isso se faz, mas há uma demanda social por essa certeza, por essa segurança, por essa informação, por essa clareza, por essa transparência.

O mundo digital e a Lei de Proteção de Dados

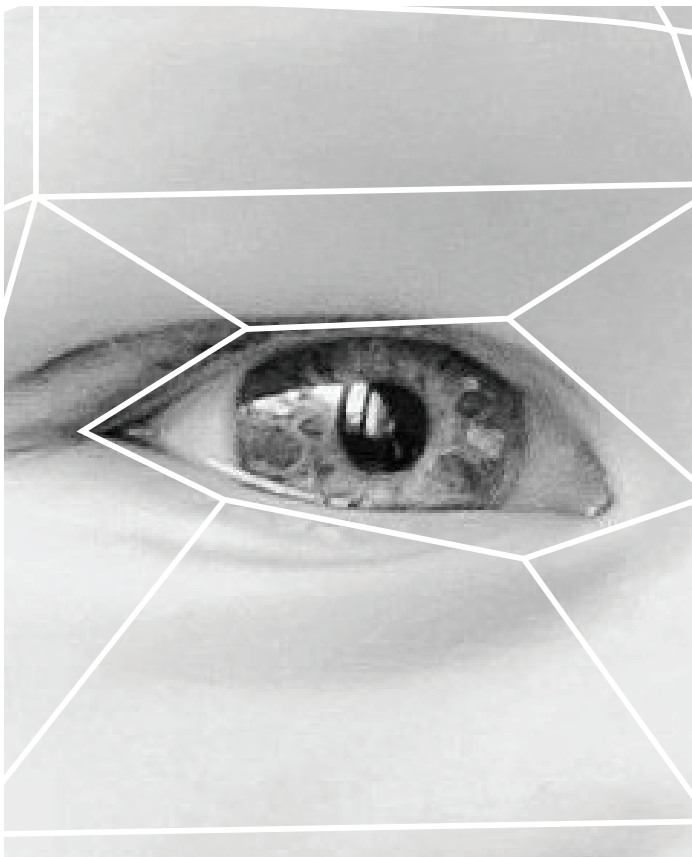
Agora eu entro no mundo digital, no tema da Lei de Proteção de Dados e trouxe essa imagem para começar. Eu queria trazer um pouco dessas sensações novas que os meios digitais nos trazem. Nas palestras de ontem já se alertou bastante sobre os perigos que vivemos no mundo digital, as mudanças pelas quais passamos, e eu queria trazer isso para relacionar com a pessoa, que é o tema desta palestra.

Às vezes eu olho para essa imagem e sinto uma coisa negativa, noutras uma coisa positiva. Você pode imaginar que essa pessoa (uma criança?) está se decompondo, se desfazendo – isso é uma visão negativa. É meio triste você imaginar que a gente está se despedaçando, se fragmentando. Mas você também pode imaginar que a gente está se formando, que esses quadradinhos estão indo em direção à pessoa, estão formando a identidade da pessoa.

Hoje temos o celular na palma das mãos e isso nos dá a sensação de que nós dominamos a tecnologia. Mas precisamos ter consciência de que a tecnologia também nos domina. E ter a humildade de reconhecer que esses aparelhinhos podem estar nos manipulando, que estamos perdendo autonomia, estamos perdendo nossa individualidade.

Isso pode estar acontecendo sem percebermos, porque estamos maravilhados com os benefícios. Eu não tenho uma visão catastrófica, gostei muito de ouvir o corregedor-geral dizendo para não entrarmos em pânico. Eu só quero provocar essas questões com essa imagem para verificar como a identidade da pessoa está hoje ligada no mundo digital. Adolescentes se suicidam porque o seu perfil na rede social ficou mal; a vida dele estava normal, mas o perfil na rede social foi destruído e a identidade que ele tem com aquele perfil virtual é tão intensa que o leva a cometer esse ato extremo.

Mas podemos imaginar aqui uma terceira hipótese,



que a pessoa não está se decompondo nem se construindo, mas que essa pessoa está migrando. Uma pessoa que está no mundo real, mas também está nas redes, também está no mundo digital.

A vida no mundo digital é uma nova realidade. Tem soluções maravilhosas, mas também tem problemas assombrosos, se for feito um mau uso desse poderio que são os dados hoje. Então é preciso ter consciência dos novos problemas, mas sem desespero, sem pânico. É preciso ter consciência para saber como lidar com os novos desafios, com as novas tecnologias.

Muitos analistas dizem que os dados são o novo petróleo, mostrando a importância dos dados para a economia. Fala-se da economia movida a dados. Penso que a LGPD veio em muito boa hora nos dar ferramentas para lidar com essa nova realidade. Ela não tem todas as respostas, mas ela tem muitas ferramentas, muitos conceitos, um aparato teórico, muitas novidades que devemos utilizar para repensar as nossas atividades. No meu caso, as atividades do Registro Civil das Pessoas Naturais e os registros públicos.

LGPD: proteção contra o processamento indevido dos dados

A primeira grande sacada da lei que me chamou atenção nos estudos que fiz é que a Lei Geral de Proteção de Dados, além da privacidade, dá proteção contra o processamento indevido dos dados.

Portanto, a LGPD não protege só a privacidade. O registro público sempre protegeu a privacidade, sabemos lidar com isso. A LGPD protege contra o processamento indevido. O processamento massivo de dados e as inferências que se faz desse processamento é uma grande novidade dos nossos tempos.

A tecnologia mudou. Pela simples mudança do meio, há facilidade de se acessar uma informação, por exemplo, um processo judicial. A facilidade de acessar a informação num processo judicial é muito grande. Aquela verdade aprendida na faculdade de direito – de que o processo era público, salvo os casos de segredo de justiça – também se modificou.

Isso não existe mais, os processos foram para o mundo digital. A possibilidade de manipular o processo e suas informações é muito grande com as ferramentas de tecnologia da informação. Então a publicidade do processo foi mitigada, e hoje não se pode ter acesso a qualquer processo judicial, mesmo que eles sejam públicos. Ou seja, não estamos protegendo apenas a privacidade, mas colocando um freio no processamento massivo de dados.

LGPD e a garantia da igualdade, liberdade e democracia

A Lei Geral de Proteção de Dados protege o princípio da igualdade. Qual o bem jurídico ali protegido? “Não são dados, não é tecnologia, são pessoas”. E os algoritmos estão trabalhando com isso. Podem ser usados de maneira inadequada contra o princípio da igualdade, basta imaginar que esses algoritmos trabalham com estatísticas, com as repetições de dados, e se temos, por exemplo, padrões discriminatórios na sociedade, que agridem minorias, esses padrões discriminatórios vão se replicar nos algoritmos e até acentuá-los. A tendência será então perpetuar a discriminação, a desigualdade.

Mas esse caso seria de mau uso. Não é regra que o processamento massivo vai causar discriminação, é uma tendência, um efeito colateral, digamos assim. É por isso que temos agora uma lei para nos proteger. Protege a nossa liberdade. Eu estava refletindo sobre isso. A proteção da privacidade é uma proteção da nossa liberdade. Mesmo fora das redes, a proteção da privacidade é uma proteção

da livre manifestação da nossa personalidade, das nossas ideias, com tranquilidade, com independência.

Nessa sociedade de vigilância podemos até deixar de comprar algo, como um remédio para impotência sexual, para não deixar rastros, para não sermos vigiados. Não queremos esse controle.

Eu gostei muito da palestra do doutor Alves Braga, ele fez aquela pergunta provocativa no final – se estamos diante do fim da privacidade, se é possível termos privacidade no mundo hiperconectado. E penso que não vou responder, claro, mas oferecer uma tentativa de resposta até para homenageá-lo, dizer as reflexões que fiz e que me foram proporcionadas pela brilhante palestra que nos deu.

Lembrei o seguinte, numa cidadezinha de 15 mil habitantes não havia privacidade. Eu trabalhei no cartório de uma cidade muito pequena, 15 mil habitantes, e eles sabiam quando eu estava no cartório, quando eu não estava. Eles sabem se você está em casa ou se você não está, simplesmente porque as pessoas passam na porta e veem a luz acesa ou o cadeado no portão. Havia muitos olhos em cima de nós, em cidades pequenas existe isso, depois a conversa à toa espalha essa informação. Não estou nem falando de fofocas maldosas, mas simplesmente do hábito de jogar conversa fora e falar sobre o que se viu e fez no dia.

Eu penso que a proteção à privacidade não é um bloqueio contra a informação pessoal. Muitas vezes teremos que nos contentar com o sigilo, para que as pessoas que saibam desses atos e fatos privados simplesmente deem o devido respeito. É como os segredos de família, é algo que todo mundo sabe, mas ninguém pode falar no assunto. Acho que a privacidade, ainda que seja maleável, porosa ou dinâmica, vai mudando, mas não deixará de existir, ela vai estar sempre presente, porque é um desejo, um valor ligado a outros valores, todos da igualdade, da liberdade.

A Lei de Proteção de Dados vai garantir também a democracia. Basta pensar que a liberdade de manifestar uma opinião política é um dado sensível. Mesmo que a pessoa não tenha Facebook, ou Instagram, provavelmente tem WhatsApp, tem um *smartphone* que vai saber sua localização. Nós nunca temos a garantia de que o microfone do celular não está ligado gravando dados. Hoje as ferramentas de informática convertem a voz em texto com facilidade e rapidez tremendas.

Então, temos essa amplitude da Lei Geral de Proteção de Dados que não diz respeito apenas à privacidade, mas

é contra o processamento indevido para a garantia da igualdade, liberdade, democracia.

Esse foi o recorte que eu fiz, mas há muitos outros recortes para se ver a dimensão do que estamos estudando. E espero que no Brasil venha a ser reconhecida a proteção de dados como um direito fundamental da pessoa.

LGPD e a titularidade dos dados pessoais: quem forma banco de dados não pode usar, fruir e dispor desses dados

A titularidade dos dados pessoais é outra grande sacada da lei para atingir seus objetivos. É muito difícil garantir isso porque estamos lidando com empresas muito poderosas, muito grandes, que têm algoritmos, que tratam os dados. Como enfrentar esse poder? Com a ferramenta jurídica, parece simples, mas é fantástico. Quem é o titular dos dados pessoais? É a pessoa a quem os dados se referem. Somos todos nós, cada um de nós. Nós somos os titulares dos dados pessoais. E isso devolve para a pessoa o poder que está concentrado nas grandes corporações, pelo menos em tese.

O controle sobre os dados é da pessoa, a lei dá o direito de eliminação, de bloqueio, de saber o que foi feito com o dado. Se isso vai ser possível de operacionalizar ou não é uma questão interessante. Mas é dar o poder para quem tem que ter o poder, que somos nós, os seres humanos, cada um de nós. E a lei fez isso, escreveu muito claramente:

Art. 17. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei.

No início da Lei também estão expostos os conceitos, onde se lê que o titular dos dados é toda pessoa identificada ou identificável a que o dado se refere. É a pessoa a quem o dado se refere. Um conceito amplo. Temos que nos familiarizar com a técnica da lei, que tem trechos muito mal escritos.

O professor e magistrado Fernando Tasso comentou ontem sobre o compartilhamento de dados. Realmente o texto legal está muito mal escrito, mas é melhor termos bons juízes do que boas leis. Eu fico feliz por estar aqui na Escola Paulista da Magistratura e verificar como a instituição está estudando, se dedicando ao tema, e fico muito tranquilo como cidadão.

A lei escolheu o termo “titularidade dos dados pessoais”, que é conceito mais amplo do que propriedade,

abrangendo-a. Isso dá efeito *erga omnes*. O titular dos dados pessoais vai poder buscar o seu dado onde quer que ele esteja. Essa titularidade abrange o aspecto patrimonial e extrapatrimonial dos dados. Disso decorre a necessidade de consentimento para tratamento dos dados pessoais.

Ontem foi dito aqui várias vezes que o consentimento não é hierarquicamente superior aos outros critérios legais que legitimam o tratamento dos dados pessoais. Eu concordo com isso. Do ponto de vista legal estão todos na mesma hierarquia, o consentimento, o legítimo interesse, previsão legal etc. Mas, do ponto de vista da proteção dos direitos humanos, o critério do consentimento expressa esse conceito. Com consentimento você pode fazer qualquer coisa, até mesmo quanto a dados sensíveis, porque a pessoa é titular dos dados e quem define os limites da privacidade dos dados dela é ela mesma, ela tem essa autonomia.

Eu tirei uma conclusão a respeito da LGPD. Quem forma um banco de dados não poderá usar, fruir e dispor livremente de tais dados, pois deverá seguir as regras da LGPD, e o respeito ao verdadeiro titular dos dados, que são as pessoas a quem os dados se referem. Ainda que todos os esforços e investimentos para formar o banco de dados seja de um particular, ele não poderá livremente usar, gozar e dispor de tais dados, pois haverá de respeitar o verdadeiro titular dos dados, respeitar os limites impostos pela LGPD.

LGPD: tratamento de dados pessoais de acesso público deve considerar a finalidade

E aí, puxando a brasa para a minha sardinha, que são os cartórios, eu vou dizer que sempre fizemos isso. Desde que assumimos o cartório, temos essa consciência. Temos uma atividade delegada pelo poder público, sabemos que aquele acervo não é nosso, é público. Até para orientar os funcionários da importância do acervo costuma-se lembrar que os livros e documentos dos cartórios não são apenas papéis, mas são direitos das pessoas, de todas as pessoas. É um acervo público nesse sentido, que é de todas as pessoas. Não é público no sentido de que é propriedade do Estado. E agora temos essas regras da publicidade do acervo.

Quando eu assumi o cartório, muito tempo atrás, eu tive a companhia de um tabelião da cidade, Comarca de Patrocínio Paulista, o doutor José Henrique do Nascimento; ele me ensinou coisas que não estavam nos livros. Nós almoçávamos juntos e um dia ele perguntou: “Mar-

celo, onde é que você põe o lixo do cartório?”. “Lixo? Eu ponho num saco preto, na rua, e o lixeiro leva”. Então ele disse: “Você tem trituradora?”. “Não. O antigo interino não gostou muito que eu assumi o cartório e levou todas as máquinas que fossem possíveis levar, menos os livros, que ele deixou bem preservados, talvez por consciência da importância coletiva dessa base de dados”.

E assim fui aprendendo cada vez mais, que temos que tomar cuidado até com o lixo produzido no cartório. Tiramos uma cópia para fazer autenticação, às vezes, ela fica ruim. E é um contrato particular, é preciso cuidado com essa cópia. Não se pode simplesmente guardar para usar o verso. De repente você usa o verso para fazer uma anotação, entrega para outra pessoa, e aquela informação pessoal vazou sem o uso de eletrônica. Era no papel mesmo, por conta de uma cópia.

Então, já temos esse cuidado, essa prática nos cartórios. E talvez pudéssemos pensar que a LGPD não se aplicaria ao cartório porque os dados são públicos. Mas a lei foi muito clara, muito didática, para dizer que “o tratamento de dados pessoais, cujo acesso é público, deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização” (art. 7º, § 3º).

Já está muito claro, mas reafirmo, essa lei se aplica aos cartórios, evidentemente. Não tem dúvida, e não temos aquela desculpa de que o dado que está no cartório é público, então ele pode ser publicizado. A lei é muito clara nesse aspecto. O tratamento de dados pessoais cujo acesso é público – temos a Lei de Registros Públicos dizendo que o acesso é público – deve considerar a finalidade. Por isso eu resgatei a finalidade; no nosso caso aqui, a segurança jurídica, a publicidade dos atos.

Finalidade protegida pelo direito: segurança e certeza de atos jurídicos

Essa segurança é o foco do registro público. A LGPD traz as hipóteses em que o tratamento de dados pessoais pode ser realizado. O professor Bruno Bioni disse que são dez hipóteses. Eu peguei o rol legal mais rigoroso, de tratamento de dados pessoais sensíveis, e vi que sem fornecimento de consentimento do titular, o controlador pode usar os dados no cumprimento de obrigação legal. Então eu acho que o nosso caso é esse.

O Registro Civil das Pessoas Naturais tem muitos dados pessoais, a maior parte deles é sensível. Nós trabalhamos sem fornecimento de consentimento. Muitas vezes, compartilhamos esses dados com o Poder Público, fornecemos certidões para qualquer pessoa

“O RCPN tem dados pessoais sensíveis. Trabalhamos sem obter consentimento. Compartilhamos dados com o Poder Público, fornecemos certidões. Por quê? Cumprimento de obrigação legal.”

que nos pede. Por que fazemos isso? Cumprimento de obrigação legal. A Lei de Registros Públicos obriga-nos a dar essas informações.

Eu fiquei com uma dúvida, porque a LGPD fala em obrigação “legal ou regulatória pelo controlador”, e como essa lei é tão ampla, eu não sei se a expressão “regulatória” abarcaria as normas da Corregedoria, que não é exatamente uma agência reguladora no sentido estrito. Mas é um debate desnecessário, porque os registradores tem a obrigação legal de cumprir as normas da Corregedoria, bem como estas são desdobramentos da lei, de forma que não será possível ao registrador deixar de cumprir as normas sob alegação de que a LGPD dispõe em sentido contrário. Enfim, é um debate desnecessário também porque a própria Corregedoria irá harmonizar suas normas com a LGPD.

Qual foi a lógica do art. 11 da lei? Aliás, interessante comentar essa técnica da lei, que por vezes parece irritante, pois no *caput* ela diz que tal conduta é proibida e depois vêm os parágrafos com as ressalvas. As hipóteses de exceção ao disposto no *caput* são muito extensas, amplas, abertas. Então proibiu no *caput* para quê? Mas há uma lógica nisso. A regra, então, é que não deve ser realizado o tratamento de dados pessoais. A lei escreveu dessa forma, por isso aquele rol de dez hipóteses de bases legais para tratar os dados é taxativo.

Se são exceções – essas do consentimento do titular, cumprimento de obrigação legal e muitas outras – isso me fez pensar em um vetor interpretativo. Essas exceções se interpretam restritivamente.

E aí fui reler a publicidade das notas e dos registros públicos. Nós não temos uma lei que discipline diretamente a publicidade notarial, mas dos registros públicos. A Lei 6.015/1973 estabelece no art. 16: “Os oficiais e os encarregados das repartições em que se façam os registros são obrigados a lavrar certidão do que lhes for requerido. E fornecer **às partes** as informações solicitadas”.

Por que eu grifei “às partes”? A lei menciona o conceito “partes” que é um conceito mais limitado do que

“qualquer pessoa”. O doutor Sérgio Jacomino é um visionário. Acho que já faz uns 15 anos que ele me ensinou isso.

Ou seja, agora podemos reinterpretar esse artigo dizendo que as informações só podem ser fornecidas para as partes do registro, para aquelas pessoas que estão ali diretamente relacionadas, porque são os dados delas. Para terceiros usarem a informação legal vai ser necessário um outro embasamento, outro raciocínio. Informações, não certidão. A lei tratou de forma diferente certidão e informação.

Certidão, o art. 17 complementa: “Qualquer pessoa pode requerer certidão do registro sem informar ao oficial ou ao funcionário o motivo ou interesse do pedido”.

É como o Ivan estava dizendo agora há pouco, a pessoa diz qual é o registro e recebe a certidão dele, mas não podemos emitir certidões solicitadas de forma ilimitada, sem indicação do registro, pois seriam buscas. Aplica-se o art. 16, inciso 2º, que é “fornecer informações solicitadas”.

E no Registro Civil das Pessoas Naturais, qualquer pessoa pode comparecer no cartório e perguntar quantos filhos determinada pessoa tem? É legítimo o cartório responder essa pergunta hoje?

Pela Lei 6.015 era impossível, porque o cartório não é obrigado a manter um índice pelo nome dos pais. A gente não tem onde buscar a informação da quantidade de filhos, salvo folheando todos os registros, um a um, o que seria um trabalho hercúleo. Mas, com a informatização temos essa possibilidade, podemos dar uma busca pelo campo “nome do pai”.

Então, se vem uma pessoa qualquer no cartório e solicita uma informação de quantos filhos determinada pessoa tem, o cartório pode fornecer? Acho que podemos buscar as respostas na Lei Geral de Proteção de Dados. Se a finalidade for compatível, é possível fornecer a informação. Por exemplo, estou lavrando o inventário, quero saber se o falecido tem mais filhos ou não, era um tio distante, com quem não se tinha contato, então é importante ter uma garantia de que não tem outros

herdeiros. Essa finalidade de uso da informação me parece estar compatível com a finalidade de segurança e certeza de atos jurídicos, que é o motivo pelo qual foi formalizado o registro de nascimento. No entanto, se for para outra finalidade que não esteja protegida pelo direito, que esteja em descompasso com a finalidade dos registros públicos, me parece que é o caso de recusarmos a informação.

Os tabeliães de Notas, durante muito tempo, lavraram escrituras de reconhecimento de filho porque não havia previsão de acesso a instrumentos particulares de reconhecimento de filho.

Essas escrituras de reconhecimento de filhos são públicas no sentido de acesso a qualquer pessoa? Nosso excelentíssimo corregedor-geral, na abertura deste seminário, compartilhou conosco um caso em que a Corregedoria autorizou o sigilo de um inventário porque as partes pediram. E havia patrimônio, havia dados pessoais, eles não queriam que aquelas informações ficassem acessíveis a qualquer pessoa. O pedido foi deferido. Talvez seja o caso de se normatizar essa possibilidade, em determinados casos, de as partes poderem optar por restringir a publicidade.

A certidão da escritura de testamento só é fornecida mediante comprovação de que o titular do testamento faleceu. E a escritura pública de reconhecimento de filho ainda não tem nenhuma norma. Até onde eu sei os tabeliães de Notas forneceriam a certidão da escritura com base no princípio de que as escrituras são públicas.

Eu penso que a LGPD reviu isso. Ou melhor, os operadores do direito podem rever agora essa publicidade das escrituras públicas. Porque a publicidade notarial é a publicidade da forma. O tabelião é agente público, que faz um controle público da idoneidade daquele ato, de forma imparcial e de acordo com o Direito. E as partes daquele negócio podem querer essa garantia de que o ato foi feito idoneamente, com segurança, mas podem não querer o amplo conhecimento desse ato. A publicidade, como um sistema organizado, destinado a revelar a situação jurídica a qualquer pessoa, é uma finalidade dos registros públicos, não das Notas.

O tabelião poderia trabalhar com essa questão na assessoria jurídica que ele presta: “Vocês vão querer deixar essa escritura acessível a qualquer pessoa? Restrita a tais pessoas?” As partes teriam liberdade para isso. Não vejo isso como um empecilho aos negócios, à inovação tecnológica. Pelo contrário, vejo como um incentivo. Eu

acho que mais contratos teriam essa valiosa proteção do notário, se fosse sigiloso. São coisas que podemos repensar agora, com a nova legislação e a nova realidade.

Até mesmo no Registro de Títulos e Documentos, que é um registro público e tem essa finalidade, há uma modalidade especial de registro, que é o registro para fins de conservação. Se você registra para fins de conservação, a finalidade é conservação e não aquelas outras finalidades do registro mais completas. Seria o caso de dar certidão para qualquer pessoa?

E o protesto de dívidas oriundas de contratos particulares em contrato de honorários advocatícios, por exemplo? O Tabelião de Protesto quer garantia de que aquele serviço foi executado, pede peças dos autos judiciais, comprova que aquele serviço foi executado. O ato do protesto é público, envolvendo a dívida e o credor. E os documentos que embasaram aquele protesto? Penso que não são públicos. Eles estão protegidos.

Compartilhamento da base de dados

O doutor Fernando Tasso falou bastante sobre compartilhamento no poder público ontem, então vou dizer o básico. É possível compartilhar, mas respeitando os princípios da lei: o princípio da finalidade, da adequação, e o princípio da necessidade.

Realço o princípio da necessidade, ou da minimização, pelo qual o tratamento é restrito ao mínimo necessário. O que passar disso é desproporcional, é excessivo, deve ser descartado e não mantido.

Observo também que o artigo 26 da LGPD fala em “uso compartilhado”. Isso não significa a formação de uma base única, central. O uso compartilhado deve ser muito bem delimitado pelas finalidades e competências de cada órgão. Devem ser cumpridos os princípios da LGPD. É o que está no artigo 26.

Essa mesma releitura, eu proponho que se faça com o compartilhamento de dados. Eu resgatei o artigo 49 da Lei 6.015/1973, que obriga registradores civis a enviar os dados para o IBGE.

“Art. 49. Os oficiais do registro civil remeterão à Fundação Instituto Brasileiro de Geografia e Estatística, dentro dos primeiros oito dias dos meses de janeiro, abril, julho e outubro de cada ano, um mapa dos nascimentos, casamentos e óbitos ocorridos no trimestre anterior.”

O artigo fala: “remeterão” os dados, remeterão um mapa de nascimento, casamento e óbito. No passado isso era um mapa mesmo, contendo informações que o IBGE queria, mas não era enviado o nome de ninguém.

Iam quantidades conforme as categorias e tipos que o IBGE precisava.

E agora, sob a égide da LGPD, é necessário e adequado enviar os nomes dos registrados ao IBGE? A finalidade do IBGE – finalidade pública específica de censo da população, de estatísticas – precisa dos nomes das pessoas? Hoje enviamos os nomes.

A Lei 13.846/2019 dispôs muito claramente quais são os elementos do registro que serão enviados para o INSS, ou seja, para o SIRC. Então, do registro de nascimento vamos enviar sexo, data e local de nascimento, nome completo. A lei especificou os elementos. Qual a leitura que vamos fazer, observando o princípio da necessidade? Enviar somente o que a lei determinou. O compartilhamento a ser feito está expresso na lei. É necessário enviar mais? Talvez seja. Em uma ou outra política pública, desde que justificado conforme a finalidade específica. Ou seja, aplicam-se aqueles outros critérios da LGPD que legitimam o tratamento dos dados. Em princípio, não há previsão para se transferir todos os dados.

São dois atos bem diferentes do ponto de vista operacional do sistema informático. A LGPD traz um dispositivo específico para os órgãos notariais e de registros (art. 23, § 5º):

“§ 5º Os órgãos notariais e de registro devem fornecer acesso aos dados por meio eletrônico para a administração pública, tendo em vista as finalidades de que trata o *caput* deste artigo.”

Fornecer acesso não é transferir bases de dados. E antes mesmo da LGPD, a Lei 11.977/2009, art. 41, ao tratar do registro eletrônico determinava que os cartórios deveriam “disponibilizar o acesso” ao Poder Judiciário e ao Poder Executivo. Também usa a expressão acesso. São duas leis.

Há um imperativo de ordem prática. Esses dados precisam transitar de forma eficiente e eletrônica. Os registradores civis têm ferramenta para proporcionar esse acesso. Temos a Central de Informações do Registro Civil, de âmbito nacional, regulamentada inicialmente pela Corregedoria Geral da Justiça do Estado de São Paulo. Foi uma boa ideia que virou um provimento nacional. Já é uma ferramenta para acesso de diversas autoridades da galáxia do Poder Judiciário. Não é válido o argumento de que os cartórios não tem meios de informatizar, muito pelo contrário, os cartórios já estão fazendo isso.

Eu sou registrador civil, faço parte da associação que visa defender os interesses do Registro Civil. Mas queremos defender nossos interesses não meramente

econômicos e financeiros, queremos prestar um serviço público de qualidade para a população, queremos manter nossa utilidade estratégica para o cidadão, sociedade e Poder Público. Para isso estamos constantemente nos atualizando graças a ferramentas eletrônicas que desenvolvemos, estamos interligados com a Receita Federal e emitimos CPF para todo registro de nascimento, no momento do registro, sem nenhum custo para o cidadão. Queremos cumprir as normas, dar efetividade às novidades que surgem e cumprir da melhor maneira possível, preservando o interesse do cidadão em relação à proteção dos dados pessoais, bem como compartilhando com o Poder Público dentro das regras específicas para isso e ainda mantendo todas as obrigações previstas na LGPD: resguardar as informações de quem teve acesso aos dados, acompanhar como foi feito o tratamento, enfim, garantir todos aqueles direitos. Isso não vai ser fácil, mas nós aceitamos o desafio.

Eu apresentei a imagem daquela pessoa se despedaçando ou se construindo, uma imagem forte. Agora eu ofereço outra imagem, mostrando que sou otimista, acho que a LGPD veio para o bem, para podermos viver em redes, conectados em nuvens, sem perder a tranquilidade.





Direito ao esquecimento e os Registros Públicos



Está evidente que a Lei Geral de



CINTIA ROSA PEREIRA DE LIMA

Livre-Docência em Direito Civil Existencial e Patrimonial pela Faculdade de Direito de Ribeirão Preto (USP). Pós-doutora em Direito Civil na Università degli Studi di Camerino (Itália). Doutora em Direito Civil pela Faculdade de Direito da USP.

Proteção de Dados Pessoais, doravante indicada como LGPD, (Lei nº 13.709/ 2018, com as alterações da Lei nº 13.853/ 2019) terá impacto direto e relevante nas atividades notariais e registrais.

Os tabeliães e os registradores lidam com informações pessoais cotidianamente, o que se depreende do conceito de dado pessoal trazido no art. 5º, inc. I da LGPD, considerado como a “informação relacionada a pessoa natural identificada ou identificável”. Além de realizarem tratamento de dados pessoais sensíveis, ou seja, “dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural” (art. 5º, inc. II da LGPD).

A LGPD fez questão de deixar clara a aplicação da lei às atividades notariais e registrais, explicitando tal entendimento no art. 23, aplicando às serventias extrajudiciais as mesmas regras de tratamento de dados pessoais pelo Poder Público:

§ 4º Os serviços notariais e de registro exercidos em caráter privado, por delegação do Poder Público, terão o mesmo tratamento dispensado às pessoas jurídicas referidas no *caput* deste artigo, nos termos desta Lei.

§ 5º Os órgãos notariais e de registro devem fornecer acesso aos dados por meio eletrônico para a administração pública, tendo em vista as finalidades de que trata o *caput* deste artigo.

Assim, a partir da entrada em vigor da LGPD, em agosto de 2020, as serventias extrajudiciais deverão estar adequadas aos princípios, aos direitos, às regras de tratamento de dados pessoais, sujeitando-se às consequências civis e administrativas previstas na lei.

Um desses pontos é justamente o direito ao esquecimento e o direito à desindexação.

Ao tratar do tema “direito ao esquecimento e registros públicos”, pode-se pensar *a priori* que seria um paradoxo, justamente porque uma das finalidades das atividades de registro é a publicidade consoante o art. 16 da Lei

dos Registros Públicos (Lei nº 6.015/ 1973), bem como a conservação (art. 22 da mesma lei).

Sendo assim, neste artigo far-se-á uma análise sobre o direito ao esquecimento, como direito de personalidade autônomo, bem como o direito à desindexação, como uma consequência do sistema de proteção de dados pessoais, destacando alguns pontos específicos para a concretização desses direitos na atividade registral.

1. Direito ao esquecimento

O direito ao esquecimento (*right to be forgotten*) é uma expressão vaga, de difícil conceituação. No entanto, essa terminologia já está consolidada em diversos países, *e. g.*, *right to oblivion* (inglês), *diritto all'oblio* (italiano), *derecho al olvido* (espanhol), *droit à oublier* (francês), expressões que se originam do grego *Lethe* (Λήθη, *Léthē*), significando a perda forçada da memória (PARENTONI, 2015, p. 546).

No entanto, permanece a fluidez conceitual, exigindo uma análise casuística desse direito, pois o caso concreto vai demonstrar se existem os parâmetros para aplicar esse direito de personalidade, ou seja, o resultado da ponderação de direitos: de um lado a proteção à privacidade, à identidade pessoal; e de outro, o direito à liberdade de expressão e direito à informação.

O Regulamento Geral Europeu sobre Proteção de Dados ou *General Data Protection Regulation*, doravante *GDPR*, trouxe, textualmente, no Artigo 17, o “*right to be forgotten or right to erasure*”, ou seja, “direito ao esquecimento e direito a apagar”. Entendido como o direito de se obter do responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada.

Todavia, o exercício desse direito traz um conflito entre a preservação da memória coletiva *versus* a pretensão individual ao esquecimento, o que gera muitas polêmicas sobre o tema e tem dividido opiniões.

Quanto à memória coletiva, a atividade registral tem uma função importante, tanto é assim que a Lei de Registros Públicos (doravante, LRP) traz diversos dispositivos

“É viável aplicar o direito ao esquecimento na atividade registral quando for possível preservar a intimidade, a privacidade e a identidade pessoal dos titulares dos dados pessoais sem comprometer o próprio sistema registral.”

para assegurar a conservação (arts. 22 e seguintes) e publicidade (arts. 16 e seguintes) dos atos praticados. Contudo, a própria LRP, em vários dispositivos sobre adoção, transgênero, conjugalidade dos pais na certidão de nascimento, proteção às testemunhas, em que se vislumbram mecanismos de mitigação da conservação e da publicidade registral. Por isso, é possível adiantar que é viável aplicar o direito ao esquecimento na atividade registral, não para todos os atos de registros, mas quando for possível preservar a intimidade, a privacidade e a identidade pessoal dos titulares dos dados pessoais sem comprometer o próprio sistema registral.

O direito ao esquecimento tem origem na privacidade, em especial, “o direito de ser deixado só” (*the right to be let alone*) (WARREN; BRANDEIS, 1890, p. 200). Inicialmente, o direito à privacidade tinha tal conotação; no entanto, na atual sociedade informacional, impossível manter-se isolado. Por isso, garante-se, além do direito à privacidade, o direito à autodeterminação informativa, entendida como o direito de controlar suas informações pessoais.

Contudo, o direito ao esquecimento não se resume ao direito à privacidade. Massimiliano Mezzanotte (2009, p. 81) define o direito ao esquecimento como uma situação jurídica subjetiva com *corpus* de um direito à identidade pessoal; mas *animus* de direito à privacidade. Por exemplo, uma pessoa que não queira ser estigmatizada como o condenado por um crime cometido há muitos anos atrás (identidade pessoal) precisa ter garantido o direito de que essa notícia sobre a prática de tal crime não será veiculada nos meios de comunicação de massa (privacidade).

No direito brasileiro, pode-se afirmar que o direito ao esquecimento decorre do princípio da dignidade da pessoa humana (art. 1º, inc. III CF/88), na medida em que se resguarda a honra e boa fama do indivíduo, eliminando da memória coletiva um fato que ofenda moralmente

esse indivíduo. E, mesmo nos fatos não ofensivos, tal direito decorre da dignidade da pessoa humana porque é essencial para o pleno desenvolvimento da identidade pessoal do indivíduo.

Assim, propomos conceituar o *direito ao esquecimento* como um *direito autônomo de personalidade por meio do qual o indivíduo pode excluir ou deletar as informações a seu respeito quando tenha passado um período de tempo desde a sua coleta e utilização e desde que não tenham mais utilidade ou não interfiram no direito de liberdade de expressão, científica, artística, literária e jornalística.* (LIMA, 2015, p. 515)

Ressalte-se que o direito ao esquecimento não resulta de mera justaposição do direito à identidade pessoal e do direito à privacidade; mas a aglutinação desses direitos confere ao direito ao esquecimento uma autonomia, podendo ser reconhecido como um direito de personalidade regido pelos artigos 11 e 12 do CC/2002.

Os desafios ao exercício do direito ao esquecimento se revelam na sociedade informacional, em que as informações e conteúdos multimídia são divulgados e compartilhados com muita facilidade pelas aplicações de Internet, como as redes sociais. Um exemplo sintomático é o ocorrido na primavera de 2006 (MAYER-SCHÖNBERGER, 2009, p. 02), quando uma jovem de 25 anos de idade foi impedida de se tornar uma professora em razão de sua foto com um chapéu de pirata e um copo plástico em mãos com o seguinte título “*drunken pirate*” que ela postou em sua rede social, *My Space*. Nesse caso, os dirigentes da escola entenderam que essa foto (fantasiada e com bebida aparentemente alcoólica na mão) revela uma conduta inconciliável com a missão institucional que se espera de uma professora, fato que motivou a escola a não conceder o diploma à jovem. Indignada, ela recorreu à justiça alegando violação à liberdade de expressão conforme o *First Amendment* da Constituição norte-americana; mas o Tribunal da Pensilvânia julgou favoravelmente à Universidade que denegou a concessão do diploma. (Stacey Snyder vs. Millersville University. Eastern District of Pennsylvania. J. 03/12/2008)

No Brasil, o Superior Tribunal de Justiça já consolidou o reconhecimento, em tese, do direito ao esquecimento:

[...] 5. Com efeito, o direito ao esquecimento que ora se reconhece para todos, ofensor e ofendidos, não alcança o caso dos autos, em que se reviveu, décadas depois do crime, acontecimento que entrou para o domínio público, de modo que se tornaria impraticável a atividade da imprensa para o desiderato de

retratar o caso Aida Curi, sem Aida Curi.

[...] 7. Não fosse por isso, o reconhecimento, em tese, de um direito de esquecimento não conduz necessariamente ao dever de indenizar. Em matéria de responsabilidade civil, a violação de direitos encontra-se na seara da ilicitude, cuja existência não dispensa também a ocorrência de dano, com nexos causal, para chegar-se, finalmente, ao dever de indenizar.

[...] 8. A reportagem contra a qual se insurgiram os autores foi ao ar 50 (cinquenta) anos depois da morte de Aida Curi, circunstância da qual se conclui não ter havido abalo moral apto a gerar responsabilidade civil. Nesse particular, fazendo-se a indispensável ponderação de valores, o acolhimento do direito ao esquecimento, no caso, com a consequente indenização, consubstancia desproporcional corte à liberdade de imprensa, se comparado ao desconforto gerado pela lembrança.

[...] 10. Recurso especial não provido. (REsp 1335153/RJ, Rel. Ministro LUIS FELIPE SALOMÃO, QUARTA TURMA, julgado em 28/05/2013, DJe 10/09/2013)

O caso Aida Curi trata de um brutal feminicídio ocorrido em 1958 em Copacabana, no Rio de Janeiro, e 50 anos depois, um programa sensacionalista transmitiu um documentário sobre esse acontecimento, inclusive com fotos do funeral, da família, do corpo da vítima que, à época, tinham circulado no jornal, ou seja, a fonte primária. E agora, 50 anos depois, pretendia-se resgatar esse acontecimento. O caso está em análise pelo Supremo Tribunal Federal, tendo sido reconhecida a repercussão geral: “Repercussão Geral” (art. 102, par. 3º CF/88) – tem efeito vinculante?

Ementa direito constitucional. Veiculação de programa televisivo que aborda crime ocorrido há várias décadas. Ação indenizatória proposta por familiares da vítima. Alegados danos morais. Direito ao esquecimento. Debate acerca da harmonização dos princípios constitucionais da liberdade de expressão e do direito à informação com aqueles que protegem a dignidade da pessoa humana e a inviolabilidade da honra e da intimidade. Presença de repercussão geral. (ARE 833248 RG, relator(a): min. DIAS TOFFOLI, julgado em 11/12/2014, PROCESSO ELETRÔNICO dje-033 DIVULG 19-02-

2015 PUBLIC 20-02-2015)

Outro caso importante julgado pelo STJ diz respeito à Chacina da Candelária, fato ocorrido no Rio de Janeiro em que houve diversos homicídios, porém, os acusados foram absolvidos por falta de provas. Treze anos depois, o programa Linha Direta-Justiça exibiu o caso em rede nacional, veiculando o nome e a imagem dos acusados. Nesse caso, o Ministro Relator, Luis Felipe Salomão destacou a dignidade da pessoa humana como fundamento ao direito ao esquecimento, evitando-se que a pessoa fique estigmatizada de acordo com fatos pretéritos, inviabilizando sua reinserção na sociedade e sua evolução:

[...] 2. Nos presentes autos, o cerne da controvérsia passa pela ausência de contemporaneidade da notícia de fatos passados, que reabriu antigas feridas já superadas pelo autor e reacendeu a desconfiança da sociedade quanto à sua índole. O autor busca a proclamação do seu direito ao esquecimento, um direito de não ser lembrado contra sua vontade, especificamente no tocante a fatos desabonadores, de natureza criminal, nos quais se envolveu, mas que, posteriormente, fora inocentado.

3. No caso, o julgamento restringe-se a analisar a adequação do direito ao esquecimento ao ordenamento jurídico brasileiro, especificamente para o caso de publicações na mídia televisiva, porquanto o mesmo debate ganha contornos bem diferenciados quando transposto para internet, que desafia soluções de índole técnica, com atenção, por exemplo, para a possibilidade de compartilhamento de informações e circulação internacional do conteúdo, o que pode tangenciar temas sensíveis, como a soberania dos Estados-nações.

[...]

7. Assim, a liberdade de imprensa há de ser analisada a partir de dois paradigmas jurídicos bem distantes um do outro. O primeiro, de completo menosprezo tanto da dignidade da pessoa humana quanto da liberdade de imprensa; e o segundo, o atual, de dupla tutela constitucional de ambos os valores.

8. Nesse passo, a explícita contenção constitucional à liberdade de informação, fundada na inviolabilidade da vida privada, intimidade, honra, imagem e, de resto, nos valores da pessoa e da família, prevista no art. 220, § 1º, art. 221 e no § 3º do art. 222 da Carta de 1988, parece sinalizar que, no conflito aparente entre esses bens jurídicos de especialíssima gran-

deza, há, de regra, uma inclinação ou predileção constitucional para soluções protetivas da pessoa humana, embora o melhor equacionamento deva sempre observar as particularidades do caso concreto. Essa constatação se mostra consentânea com o fato de que, a despeito de a informação livre de censura ter sido inserida no seletivo grupo dos direitos fundamentais (art. 5º, inciso IX), a Constituição Federal mostrou sua vocação antropocêntrica no momento em que gravou, já na porta de entrada (art. 1º, inciso III), a dignidade da pessoa humana como – mais que um direito – um fundamento da República, uma lente pela qual devem ser interpretados os demais direitos posteriormente reconhecidos. [...]

12. Assim como é acolhido no direito estrangeiro, é imperiosa a aplicabilidade do direito ao esquecimento no cenário interno, com base não só na principiologia decorrente dos direitos fundamentais e da dignidade da pessoa humana, mas também diretamente do direito positivo infraconstitucional. A assertiva de que uma notícia lícita não se transforma em ilícita com o simples passar do tempo não tem nenhuma base jurídica. O ordenamento é repleto de previsões em que a significação conferida pelo Direito à passagem do tempo é exatamente o esquecimento e a estabilização do passado, mostrando-se ilícito sim reagitar o que a lei pretende sepultar. Precedentes de direito comparado.

13. Nesse passo, o Direito estabiliza o passado e confere previsibilidade ao futuro por institutos bem conhecidos de todos: prescrição, decadência, perdão, anistia, irretroatividade da lei, respeito ao direito adquirido, ato jurídico perfeito, coisa julgada, prazo máximo para que o nome de inadimplentes figure em cadastros restritivos de crédito, reabilitação penal e o direito ao sigilo quanto à folha de antecedentes daqueles que já cumpriram pena (art. 93 do Código Penal, art. 748 do Código de Processo Penal e art. 202 da Lei de Execuções Penais). Doutrina e precedentes. [...]

16. Com efeito, o reconhecimento do direito ao esquecimento dos condenados que cumpriram integralmente a pena e, sobretudo, dos que foram absolvidos em processo criminal, além de sinalizar uma evolução cultural da sociedade, confere concretude a um ordenamento jurídico que, entre

a memória – que é a conexão do presente com o passado – e a esperança – que é o vínculo do futuro com o presente –, fez clara opção pela segunda. E é por essa ótica que o direito ao esquecimento revela sua maior nobreza, pois afirma-se, na verdade, como um direito à esperança, em absoluta sintonia com a presunção legal e constitucional de regenerabilidade da pessoa humana.

17. Ressalvam-se do direito ao esquecimento os fatos genuinamente históricos – historicidade essa que deve ser analisada em concreto –, cujo interesse público e social deve sobreviver à passagem do tempo, desde que a narrativa desvinculada dos envolvidos se fizer impraticável.

18. No caso concreto, a despeito de a Chacina da Candelária ter se tornado – com muita razão – um fato histórico, que expôs as chagas do País ao mundo, tornando-se símbolo da precária proteção estatal conferida aos direitos humanos da criança e do adolescente em situação de risco, o certo é que a fatídica história seria bem contada e de forma fidedigna sem que para isso a imagem e o nome do autor precisassem ser expostos em rede nacional. Nem a liberdade de imprensa seria tolhida, nem a honra do autor seria maculada, caso se ocultassem o nome e a fisionomia do recorrido, ponderação de valores que, no caso, seria a melhor solução ao conflito. [...] (REsp 1334097/RJ, Rel. Ministro LUIS FELIPE SALOMÃO, QUARTA TURMA, julgado em 28/05/2013, DJe 10/09/2013)

Esses são apenas alguns casos que demonstram que o direito ao esquecimento é bem variado, exigindo análise casuística como destacado acima.

Ademais, tais hipóteses não se confundem com a possibilidade de remoção de conteúdo gerado por terceiro em face dos provedores de aplicação de Internet, desde que seja determinado judicialmente, indicando-se a URL, prevista no Marco Civil da Internet, doravante indicada como MCI (Lei n. 12.965, de 23 de abril de 2014):

Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas



as disposições legais em contrário.

§ 1º A ordem judicial de que trata o *caput* deverá conter, sob pena de nulidade, identificação clara e específica do conteúdo apontado como infringente, que permita a localização inequívoca do material.

Não se pode confundir tal possibilidade com o direito ao esquecimento, que é mais amplo, pois se trata de um direito de personalidade autônomo que pode ou não estar relacionado com aplicação de Internet. Nos casos acima destacados, Aida Curi e Chacina da Candelária, não se trata de divulgação de conteúdo em aplicações de Internet, e sim por meio de programa de televisão. Assim, deve-se entender que a possibilidade de remoção de conteúdo pode ser uma ferramenta para a concretização do direito ao esquecimento quando, por exemplo, for necessária para inviabilizar a propagação de determinado fato.

Sobre esse ponto especificamente, há diversos julgados proferidos pelo STJ, porém exigindo-se a indicação da URL como preconiza o Marco Civil da Internet. No caso “Xuxa”, isso ficou evidente, pois o Tribunal de Justiça do Rio de Janeiro entendeu que sem indicar a URL não poderia deferir o pedido de remoção de conteúdo de qualquer correlação ao passado da atriz com sua atuação como modelo fotográfico:

APELAÇÃO CÍVEL. AÇÃO DE OBRIGAÇÃO DE FAZER. GOOGLE. PROVEDOR DE PESQUISA. FILTRAGEM PRÉVIA DAS BUSCAS. BLOQUEIO DE PALAVRAS-CHAVES. PRETENSÃO DE EXCLUSÃO GENÉRICA DE QUALQUER REFERÊNCIA QUE ENTENDA OFENSIVA À SUA HONRA OU AO SEU PASSADO DE MODELO FOTOGRÁFICO. IMPOSSIBILIDADE. NECESSIDADE DE INDICAÇÃO DO URL DA PÁGINA ONDE ESTIVER INSERIDO. DIREITO AO ESQUECIMENTO. Os provedores de pesquisa virtual não podem ser obrigados a eliminar do seu sistema os resultados derivados da busca de determinado termo ou expressão, tampouco os resultados que

apontem para uma foto ou texto específico, independentemente da indicação do URL da página onde este estiver inserido. Não está se negando à Autora o exercício do direito ao esquecimento, direito que possui de não permitir que um fato, verídico ou inverídico, ocorrido em determinado momento de sua vida, seja exposto ao público em geral, mas, afastando a responsabilidade da Ré de acordo com o entendimento firmado pelos nossos Tribunais, com base, inclusive, ao direito de informação e na ponderação entre direitos. PRECEDENTES. RECURSO DESPROVIDO. (TJRJ. Apelação Cível nº 0024717-80.2010.8.19.0209. 19ª Câmara Cível. APELANTE: MARIA DA GRAÇA XUXA MENEGHEL. APELADO: GOOGLE BRASIL INTERNET LTDA. RELATORA: DES. VALÉRIA DACHEUX.)

Nesse caso houve confusão entre direito ao esquecimento, direito à remoção de conteúdo e direito à desindexação. Exemplo: se a Xuxa quisesse impedir um documentário a seu respeito sobre o seu passado, ela poderia pedir com base no direito ao esquecimento; outra situação seria se a atriz pretendesse remover um conteúdo inserido por alguém em alguma aplicação de Internet, teria que indicar a URL conforme determina o MCI e a posição amplamente dominante no STJ; uma terceira hipótese seria se a Xuxa tivesse por objetivo desindexar o seu nome das ferramentas de busca, solicitando a instalação de filtros pelo provedor da ferramenta de busca, isso poderia ser feito com base no art. 7º, inc. VIII do MCI, pois ao se opor ao tratamento de seus dados pessoais, a atriz retira seu consentimento pedindo para não ser mais indexada nas ferramentas de busca (direito à desindexação). Entretanto, a confusão ocorre na doutrina e na jurisprudência por falta de embasamento legal que pontue especificamente cada uma dessas situações. Para evitar tal confusão, é fundamental que se compreenda o direito à desindexação, a seguir analisado.

Na hipótese de processamento de dados em massa e

“Considerada a indexação como atividade de tratamento de dados pessoais, aplica-se a LGPD que, no art. 18, traz como um direito do titular de dados pessoais a revogação do consentimento nos termos do § 5º, do art. 8º, da LGPD.”

um processamento informatizado, o direito ao esquecimento toma outros contornos e consequências ainda maiores. Por isso, o direito ao esquecimento foi trazido no Regulamento Geral Europeu como uma forma de excluir os dados ou impedir ou se opor ao processamento dos seus dados pessoais com o propósito de minimizar ao máximo as consequências ensejadas pela disseminação em massa e de maneira transfronteiriça de tais conteúdos.

A LGPD não trouxe textualmente o “direito ao esquecimento”, até porque como já foi exposto *supra*, é um direito de personalidade autônomo com *status* constitucional (dignidade da pessoa humana). No entanto, é possível que em alguns casos esses direitos se tangenciem.

Assim, cabe destacar os possíveis fundamentos na LGPD para o direito ao esquecimento, quando forem úteis as ferramentas previstas na lei para a efetivação desse direito de personalidade.

Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: [...]

IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei; [...]

VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;

Observe-se que esse artigo permite a “eliminação” dos dados pessoais, quando desnecessários, excessivos ou tratados de maneira ilícita, além dos dados tratados com o consentimento do titular. Nas atividades de registros, a conservação dos atos praticados é fundamental para a higidez do sistema registral, bem como para a segurança jurídica. No entanto, o direito ao esquecimento afetará a publicidade registral, quando possível, resguardado o direito de sigilo para determinados atos, tais como alteração de nome e gênero aos transgêneros, dentre outros.

2. Direito à desindexação

A partir do desenvolvimento da tecnologia da informação (TIC), o tratamento dos dados pessoais passou a tomar novos contornos, o exemplo em destaque são as ferramentas de busca (*search engines*). Esse tema foi objeto do caso *González vs. Google*, originado na Espanha, em que foi reconhecido que as atividades de indexação são consideradas atividades de tratamento de dados pessoais, ensejando a aplicação da lei específica sobre a matéria. Esse caso, analisado pelo Tribunal de Justiça europeu acima mencionado, foi emblemático porque a Agência Espanhola de Proteção de dados Pessoais (AEPD), em julho de 2010, entendeu que as ferramentas de busca estão sujeitas à lei de proteção de dados, sendo essa uma forma de tratamento de dados pessoais.

No caso, o cidadão espanhol, González fora processado por débitos previdenciários e tivera seus bens leiloados em razão da execução em que o leilão foi divulgado no jornal de grande circulação como determina a lei, o jornal espanhol *La Vanguardia*. Dez anos após a execução, o cidadão espanhol foi surpreendido com a indexação dessa notícia do leilão publicado no jornal *La Vanguardia* quando utilizada a ferramenta de busca *Google*. Assim, o indivíduo solicitou que o seu nome não aparecesse nos buscadores *Google* alegando não consentir com o tratamento de seus dados pessoais conforme a Diretiva 95/46/CE e a Diretiva 2002/58/CE.

Em decisão de 20 de novembro de 2007, a Agência Espanhola de Proteção de Dados, Processo nº TD/00463/2007, AEPD Res. n. R/01046/2007, estabeleceu um marco ao reconhecer que o indivíduo tem direito de seus dados não constarem das ferramentas de busca.

Mas em que consiste a prática de indexar? E tal prática pode ou não ser considerada tratamento de dado pessoal?

Essa atividade é realizada por robôs, que são copiados, organizados e selecionados posteriormente por algoritmos, sendo que os robôs ou *softwares* são programados pelos provedores da ferramenta de busca. Assim, de acordo com o *GDPR* (art. 4.2) e a LGPD (art. 5º, inc. X), considera-se tratamento de dados pessoais qualquer informação ou conjunto de operações feitas com dados pessoais, tais como coletar, salvar, organizar, estruturar, armazenar, adaptar, alterar, consultar, usar e disponibilizar por meio de transmissão, disseminação ou por outra forma deixar disponível, combinar, restringir, apagar ou destruir.

Pizzetti Franco (2014, p. 808) define o direito à indexação como: “o direito de não ver facilmente encontrada

uma notícia que não seja mais atual. O efeito principal da indexação e difusão da notícia por meio das ferramentas de busca é, de fato, colaborar de maneira contínua para a atualidade das informações e criar um perfil da pessoa a que se referem”.

A natureza desse direito, assim como o direito ao esquecimento, é um direito de personalidade; porém, o direito à desindexação está fundado na ausência do consentimento do titular dos dados que se opõe ao tratamento quando não concorda que suas informações pessoais sejam indexadas.

No Brasil, o STJ julgou um outro caso interessante em que uma pessoa prestou concurso para a magistratura no Estado do Rio de Janeiro, concurso que foi anulado por suspeita de fraude, sendo o nome dessa candidata envolvido na suposta fraude. A nosso ver se trata claramente do direito à desindexação e não remoção de conteúdo anteriormente comentada:

[...] 3. A jurisprudência desta Corte Superior tem entendimento reiterado no sentido de afastar a responsabilidade de buscadores da internet pelos resultados de busca apresentados, reconhecendo a impossibilidade de lhe atribuir a função de censor e impondo ao prejudicado o direcionamento de sua pretensão contra os provedores de conteúdo, responsáveis pela disponibilização do conteúdo indevido na internet. Precedentes. 4. Há, todavia, circunstâncias excepcionalíssimas em que é necessária a intervenção pontual do Poder Judiciário para fazer cessar o vínculo criado, nos bancos de dados dos provedores de busca, entre dados pessoais e resultados da busca, que não guardam relevância para interesse público à informação, seja pelo conteúdo eminentemente privado, seja pelo decurso do tempo. 5. Nessas situações excepcionais, o direito à intimidade e ao esquecimento, bem como a proteção aos dados pessoais deverá preponderar, a fim de permitir que as pessoas envolvidas sigam suas vidas com razoável anonimato, não sendo o fato desabonador corriqueiramente rememorado e perenizado por sistemas automatizados de busca. 6. O rompimento do referido vínculo sem a exclusão da notícia compatibiliza também os interesses individual do titular dos dados pessoais e coletivo de acesso à informação, na medida em que viabiliza a localização das notícias àqueles que direcionem sua pesquisa fornecendo argumentos de pesquisa relacionados ao fato noticiado, mas não àqueles

que buscam exclusivamente pelos dados pessoais do indivíduo protegido. 7. No caso concreto, passado mais de uma década desde o fato noticiado, ao se informar como critério de busca exclusivo o nome da parte recorrente, o primeiro resultado apresentado permanecia apontando link de notícia de seu possível envolvimento em fato desabonador, não comprovado, a despeito da existência de outras tantas informações posteriores a seu respeito disponíveis na rede mundial. (REsp 1660168/RJ, Rel. Ministra NANCY ANDRIGHI, Rel. p/ Acórdão Ministro MARCO AURÉLIO BELLIZZE, TERCEIRA TURMA, julgado em 08/05/2018, DJe 05/06/2018)

Nesse caso, houve uma divergência entre a Relatora Ministra Nancy Andrigli que foi contrária ao deferimento do pedido, pois conforme o MCI dever-se-ia indicar a URL (como uma espécie de direito ao esquecimento mitigado); assim, a Ministra destacou que o julgamento desse caso restou semelhante ao precedente europeu (antes aqui neste artigo comentado), mas ressaltou que o Brasil ainda não tinha (à época) uma Lei Geral de Proteção de Dados Pessoais.

Entretanto, os demais ministros acompanharam o voto divergente do Ministro Marco Aurélio Bellizze, para quem a questão refere-se à proteção de dados pessoais e não de remoção de conteúdo, exigindo um tratamento diferenciado pela Corte. Assim, o Ministro Bellizze destacou:

“Por outro vértice, aqueles que quiserem ter acesso a informações relativas a fraudes em concurso público, não terão seu direito de acesso impedido, porquanto as fontes que mencionam inclusive o nome da recorrida permanecerão acessíveis. Contudo, sua busca deverá conter critérios relativos a esse conteúdo, seja em conjunto com o nome da recorrida, seja de forma autônoma. Tem-se, assim, uma via conciliadora do livre acesso à informação e do legítimo interesse individual, porque não serão excluídos da busca referências ao nome da recorrida, nem serão ocultados definitivamente os resultados advindos de uma busca que faça referência a seu nome em conjunto com termos que remetam ao resultado hoje exibido. O que se evitará é, tão somente, que uma busca direcionada a informações sobre a sua pessoa, por meio da inclusão de seu nome como critério exclusivo de busca, tenha por resultado a indicação do fato desabonador noticiado há uma década, impedindo a superação daquele momento.”

Considerada a indexação como atividade de tratamento de dados pessoais, aplica-se a LGPD que, no art. 18, traz como um direito do titular de dados pessoais a revogação do consentimento nos termos do § 5º, do art. 8º, da LGPD. Assim, quando uma determinada pessoa solicita que não seja mais indexada nas ferramentas de busca, exerce seu direito de revogação do consentimento, se considerarmos que as ferramentas de busca se sujeitam a um sistema *opt-out*.

3. Aplicação do direito ao esquecimento e do direito à desindexação na atividade registral

A questão-problema colocada neste artigo é sobre a (in) aplicabilidade do direito ao esquecimento e do direito à desindexação pelos oficiais de registro. Inicialmente parece um paradoxo, pois dois princípios dos registros públicos, que colocam em xeque o direito ao esquecimento e o direito à desindexação, são justamente o princípio da conservação e o princípio da publicidade. Entretanto, não existem direitos absolutos, além de a própria LRP excepcionar a publicidade em alguns atos de registro, como o caso da adoção, por exemplo, art. 95, parágrafo único da LRP, capítulo XVII das NSCGJ (itens 117 e 129) e Provimento nº 63 do CNJ.

Nesse sentido, parte da doutrina, como Walter Ceneviva (2010, p. 89), entende que todos os atos de registros devem permanecer abertos permanentemente para que todos deles possam tomar conhecimento; muito embora o próprio autor destaque existir algumas exceções. Assim, Walter Ceneviva afirma ser estranho a LRP não ter mencionado a “publicidade” em seu art. 1º; no entanto, acreditamos que tal omissão foi proposital haja vista as exceções.

Ademais, destacam-se as funções do registro público, ou seja, a segurança jurídica e cognoscibilidade dos atos inscritos nos termos do art. 1º da Lei nº 8.935/1994 e art. 1º da LRP. Portanto, caberá realizar a ponderação de valores, como bem destacado pelo Ministro Bellizze no julgamento anteriormente citado, para compatibilizar os princípios e as funções dos registros públicos com o direito ao esquecimento e à desindexação.

Dois exemplos práticos deixam tal necessidade evidente. Um é o caso dos transgêneros, que nos termos do art. 5º do Provimento do CNJ 73/2018 tem natureza sigilosa. O sigilo foi confirmado no Provimento nº 16/2018 da Corregedoria Geral da Justiça do Estado de São Paulo (art. 10). Nesses casos a publicidade deve ser mitigada, pois a emissão de certidão deve ser feita somente por

resumo. No entanto, permanece uma questão de difícil solução: se antes de alterar o gênero e o nome, a pessoa tem imóveis e na matrícula consta sua qualificação anterior, o que fazer depois da alteração de gênero e nome: poderia se excluir tais informações, abrindo uma nova matrícula? São questões que o CNJ e/ou a Corregedoria Geral da Justiça deverão normatizar.

Outro caso é a publicação de editais *online* prevista nas Normas de Serviço da Corregedoria Geral da Justiça do Estado de São Paulo, capítulo XX, art. 428.1.8, que ocorre nas execuções de contratos de alienação fiduciária, retificação de registro de imóveis, registro de loteamentos, desmembramentos e bens de família. Contra a fonte primária, no caso o IRIB que organiza a publicação desses editais, cuja publicidade é exigida por lei, não há que se opor o direito à indexação. Contudo se tal informação for relacionada nos *sites* de busca, então o titular poderá pleitear contra as ferramentas de busca a desindexação como ocorreu no caso *González vs. Google*, bem como no caso julgado pelo STJ em 2018, para desindexar o nome de uma pessoa de notícia sobre possível fraude no concurso público.

Conclusão

Os diversos desafios na sociedade informacional para o desenvolvimento da pessoa humana são cada vez mais complexos. Todavia, a dignidade da pessoa humana (art. 1º, inc. III da CF/1988) exige um olhar cuidadoso sobre essas questões pelo aplicador do direito. O direito à proteção de dados pessoais deve ser considerado um direito e garantia individual. Nesse sentido, os oficiais de registro, realizando a ponderação de valores, poderão, a depender do caso concreto, aplicar o direito ao esquecimento desde que não comprometa a higidez do sistema registral.

No que diz respeito ao direito à desindexação, tal direito é oponível às ferramentas de busca, uma vez que no caso os oficiais de registro não desempenham tal função, por isso, não respondem pelo direito à desindexação.

Em suma, os §§ 4º e 5º do art. 23 da Lei nº 13.709/2018 deixam claro que a LGPD se aplica às serventias extrajudiciais. Nesse sentido, devem ser reconhecidos o direito ao esquecimento e o direito à desindexação, este último relacionado diretamente à proteção dos dados pessoais, na medida em que indexar é tratamento de dados pessoais.

Entretanto, não existem direitos absolutos, o que resultará que em determinadas situações o oficial de regis-

tro deverá primar pela publicidade registral; em outras, ao contrário, pelo direito ao esquecimento. Todavia, as Normas de Serviço das Corregedorias estaduais devem padronizar os procedimentos a serem adotados dada a prudência registral.

Quanto ao direito à desindexação, a publicação de editais *online* prevista nas Normas de Serviço da Corregedoria Geral da Justiça do Estado de São Paulo, capítulo XX, art. 428.1.8, que ocorre nas execuções de contratos

de alienação fiduciária, retificação de registro de imóveis, registro de loteamentos, desmembramentos e bens de família deve ser analisada com atenção.

No caso, o IRIB deve ser considerado fonte primária, pois organiza a publicação desses editais, cuja publicidade é exigida por lei, não lhe sendo oponível o direito à indexação. Contudo, se tal informação for relacionada nos sites de busca, então o titular poderá pleitear contra as ferramentas de busca à desindexação.

Referências bibliográficas

- CASTELLS, Manuel. *The information age: economy, society and culture*. Vol. I: *The rise of the network society*. Malden (MA): Blackwell Publishers, 2000.
- _____. *The power of Identity*. 2 ed. Malden (MA): Blackwell Publishers, 2007.
- DE SOUSA, Rabindranath V. A. Capelo, *O Direito Geral de Personalidade*, Coimbra: Coimbra Editora, 1995.
- CENEVIVA, Walter. *Lei dos Registros Públicos Comentada*. 20 ed. São Paulo: Saraiva, 2010.
- _____. *Lei dos Notários e dos Registradores Comentada*. 8 ed. São Paulo: Saraiva, 2010.
- EASTERN DISTRICT OF PENNSYLVANIA. *Stacey Snyder vs. Millersville University*. J. 03/12/2008.
- GOMES, Orlando. *Introdução ao Direito Civil*. 18 ed. Rio de Janeiro: Forense, 2001.
- PERLINGIERI, Pietro. *Manuale di Diritto Civile*. 6. ed. Napoli: Edizioni Scientifiche Italiane, 2007.
- LIMA, Cíntia Rosa Pereira de. La dinamicità del diritto all'oblio e il pericolo della sua non flessibilità secondo l'orientamento del Supremo Tribunale Federale brasiliano. In: DE CICCO, Maria Cristina; PINTO, Eduardo Vera-Cruz; SILVA, Marco Antônio Marques da (orgs.) *Direito à verdade, à memória e ao esquecimento*. Lisboa: AAFDL, 2017. pp. 317 – 332.
- _____. Direito ao esquecimento e internet: o fundamento legal no Direito Comunitário Europeu, no Direito Italiano e no Direito Brasileiro. In: CLÊVE, Clémerson Merlin; BARROSO, Luis Roberto. *Coleção Doutrinas Essenciais em Direito Constitucional: direitos e garantias fundamentais*, volume VIII, São Paulo, Revista dos Tribunais, 2015, p. 511 – 544.
- _____. DE LUCCA, Newton; SIMÃO FILHO, Adalberto; MACIEL, Renata Mota (coords). *Direito & Internet IV: Sistema de Proteção de Dados Pessoais*. São Paulo: Quartier Latin, 2019.
- _____. DE LUCCA, Newton; SIMÃO FILHO, Adalberto (coords). *Direito & Internet III: Marco Civil da Internet – Lei n. 12.965/2014*. São Paulo: Quartier Latin, 2015. (tomos I e II).
- _____. PEROLI, Kelvin. *Direito Digital: compliance, regulação e governança*. São Paulo: Quartier Latin, 2019.
- MAZUR, Maurício. A dicotomia entre os direitos de personalidade e os direitos fundamentais. In: MIRANDA, Jorge; RODRIGUES JÚNIOR, Otavio Luiz; FRUET, Gustavo Bonato. (orgs.) *Direitos da Personalidade*. São Paulo: Atlas, 2012. pp. 25 – 64.
- MEZZANOTTE, Massimiliano. *Il diritto all'oblio: contributo allo studio della privacy storica*. Napoli: Edizioni Scientifiche Italiane, 2009.
- MOARES, Maria Celina Bodin. Sobre o Nome da Pessoa Humana. In: *Revista da EMERJ*. Nº 12, 2000, p. 71.
- PIZZETTI, Franco. *Privacy e il diritto europeo alla protezione dei dati personali: dalla direttiva 95/46 al nuovo Regolamento europeo*. Torino: G. Giappichelli Editore, 2016. p. 20.
- _____. Le Autorità Garanti per la Protezione dei Dati Personali e la Sentenza della Corte di Giustizia sul Caso Google Spain: è Tempo di Far Cadere il “Velo di Maya”. In: *Il Diritto dell'informazione e dell'informatica*, 2014, fasc. 4-5, Giuffrè, pp. 805 – 829.
- MAYER-SCHONBERGER, Viktor. *Delete: the virtue of forgetting in the Digital Age*. New Jersey: Princeton University Press, 2009.
- PARENTONI, Leonardo Netto. O direito ao esquecimento (right to oblivion). In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coords). *Direito & Internet III: Marco Civil da Internet – Lei n. 12.965/2014*. São Paulo: Quartier Latin, 2015. Tomo I. pp. 539 – 618.
- RODOTÀ, Stéfano. *I diritti della personalità*. Milão: Giuffrè, 1950.
- _____. Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali. In: *Rivista Critica del Diritto Privato*, anno XV, n. 1, março 1997, pp. 583 – 609.
- SOLOVE, Daniel. J. Conceptualizing Privacy. In: *California Law Review*, vol. 90, Issue 4 (2002), pp. 1087 – 1156.
- SUPERIOR TRIBUNAL DE JUSTIÇA. REsp 1335153/RJ, Rel. Ministro LUIS FELIPE SALOMÃO, QUARTA TURMA, julgado em 28/05/2013, DJe 10/09/2013.
- _____. REsp 1334097/RJ, Rel. Ministro LUIS FELIPE SALOMÃO, QUARTA TURMA, julgado em 28/05/2013, DJe 10/09/2013.
- _____. REsp 1660168/RJ, Rel. Ministra NANCY ANDRIGHI, Rel. p/ Acórdão Ministro MARCO AURÉLIO BELLIZZE, TERCEIRA TURMA, julgado em 08/05/2018, DJe 05/06/2018.
- SUPREMO TRIBUNAL FEDERAL. ARE 833248 RG, relator(a): min. DIAS TOFFOLI, julgado em 11/12/2014, PROCESSO ELETRÔNICO dje-033 DIVULG 19-02-2015 PUBLIC 20-02-2015.
- TRIBUNAL DE JUSTIÇA DO RIO DE JANEIRO. Apelação Cível nº 0024717-80.2010.8.19.0209. 19ª Câmara Cível. APELANTE: MARIA DA GRAÇA XUXA MENEGHEL. APELADO: GOOGLE BRASIL INTERNET LTDA. RELATORA: DES. VALÉRIA DACHEUX.
- WARREN, Samuel D.; BRANDEIS, Louis D. The Right to Privacy. In: *Harvard Law Review*, v.4, pp. 193 – 220, 1890.



A publicidade jurídico- registral, seu objeto e veículo de sua difusão



O tema é bastante importante, vamos



RAFAEL RICARDO GRUBER
6º Oficial de Registro de Imóveis de São Paulo (SP)

focar mais a questão da publicidade jurídico-registral, qual o objeto dessa publicidade, e qual é o veículo pelo qual se faz a difusão desses dados submetidos ao registro.

O que é essa publicidade dos registros públicos? É a mesma publicidade dos atos administrativos? Ou é a mesma publicidade do ato notarial, por exemplo? A resposta é negativa: não é a mesma publicidade.

A publicidade dos atos da Administração Pública, por exemplo, é regrada pelo direito administrativo. A publicidade registral está ligada ao direito privado, ao direito civil, e está intimamente ligada com o direito de propriedade.

É dessa publicidade registral que se extrai o que se chama de cognoscibilidade, a possibilidade de um terceiro ou de qualquer pessoa conhecer uma situação jurídica sujeita a registro – é ela que fundamenta a possibilidade de que existam direitos reais, direitos que sejam oponíveis contra todos, e não somente às partes que contrataram.

Então, há uma situação muito profunda, muito séria, da publicidade quando se fala em registros públicos, porque ela está ligada à cognoscibilidade. E essa cognoscibilidade é o que permite gerar a oponibilidade, é o que permite gerar a eficácia real dos direitos.

Se existe propriedade, se existe direito real, e se eu posso coagir um terceiro que não participou de um negócio jurídico comigo a respeitar meu direito de propriedade é porque ele pode conhecer a minha situação jurídica. Sem uma situação jurídica organizada, que permita constatar quem é o titular daquela situação jurídica, não poderíamos fundamentar o direito real.

Mas como tratar uma situação em que se tem de um lado a privacidade, a necessidade de proteger dados pessoais, especialmente com o avanço da tecnologia, e de outro se tem a necessidade de cognoscibilidade, de a publicidade ser acessível a quem possa interessar para que um direito real possa manter sua força?

O artigo 16 da Lei de Registros Públicos, que é de 1973, é bastante abrangente no que diz respeito à obrigação de um oficial de registro de dar acesso às informações. Os oficiais e os encarregados das repartições em que se façam os registros são obrigados a fornecer certidão do que lhes for requerido e a fornecer às partes

as informações solicitadas.

Eu achei interessante quando em outra palestra o colega mencionou a expressão “partes” como se pudessemos fazer a ressalva de a quem vamos dar uma informação. Na verdade, mesmo no Registro de Imóveis damos informação verbal, por exemplo, e não somente para a parte.

Qual a diferença ontológica de informação ou de certidão? A certidão é documentada, é instrumentalizada de alguma forma. E a partir dela, vai existir fé pública de uma informação que consta no registro.

Diferentemente, a informação é prestada quando a parte dispensa a certidão, ou seja, ela não precisa de uma prova, de um instrumento para fazer prova daquela situação. Para ela basta ter informação: “eu quero saber se o fulano tem imóvel.” Sim ou não, é uma informação. E nós entendemos que somos obrigados a prestar essa informação, porque a lei assim exige.

É interessante pensar o seguinte: quando essa lei foi editada, quem já trabalhava no cartório, lá em 1976, lembra das máquinas de escrever. A pessoa ia até o balcão do cartório, nós abríamos aqueles gavetões com os indicadores para fazer a busca, batíamos à máquina a informação e pronto.

Para aquela época sem tecnologia, o art. 16 estava perfeito. E hoje, 40 e poucos anos depois? Como está essa situação? Esse artigo de lei se mantém assim? Hoje, uma pessoa com celular vai direto à informação. Então, naquela época ter acesso à informação não era uma coisa tão impactante.

A evolução tecnológica e social

Hoje, uma pessoa pode ter acesso à informação ampla de maneira desregrada. Com um celular ela consegue acesso à planta de proprietários de uma cidade inteira.

A grande questão, ainda que não existisse a LGPD, é que deveríamos pensar numa situação de evolução tecnológica e social. A evolução foi mencionada aqui ontem, alguma coisa do Miguel Reale sobre fato, valor e norma.

Qual o nosso fato social em 2020, em relação ao que tínhamos em 1973? É a mesma situação? Não é. A lei deixou isso expresso: não é mais a mesma situação, porque a LRP dispôs que qualquer pessoa pode requerer a certidão do registro sem informar o motivo ou o interesse do pedido. Qualquer pessoa pode pedir a certidão sem dizer por que. Tem direito a essa informação. Será que isso ainda tinha sentido depois da Constituição de 1988, especialmente agora depois da LGPD?

E aqui, a forma de certidão. Hoje em dia, no Registro de Imóveis, a certidão de inteiro teor é a que mais prevalece, aquela cópia reprográfica da matrícula com todo o histórico desde quando aberta a matrícula, com toda a informação.

No Registro de Imóveis, a informação em resumo é raríssima. Algumas pessoas chegam hoje no cartório e pedem a certidão da seguinte forma: “Diga, ao final, quem é o proprietário atual e quais são os ônus especificamente”. E nós fornecemos a certidão dizendo isso, mas é preciso um cuidado extremo.

No futuro, com o registro eletrônico, a tendência é que cada vez mais tenhamos que dar a certidão de direitos e de situações jurídicas ativas e atuais. Vamos ter que dizer a situação jurídica atual de um bem, não importa o histórico. Mas então, em relatório, a pessoa pode dizer qual informação ela quer e o oficial deve indicar isso de maneira precisa.

O parágrafo primeiro da LRP diz que a certidão de inteiro teor poderá ser expedida por meio datilográfico ou reproográfico. Interessante o nosso estado da arte de tecnologia naquele momento. Era bacana ter uma máquina Xerox, a fotocópia era incrível. Datilografar também era uma coisa muito boa, era melhor que fazer manuscrito. Grande parte dos registros, à época, ainda eram feitos na caneta.

A norma é dinâmica

Talvez se opondo ao artigo 17 da Lei 6.015/1973, o artigo 17 da LGPD estabelece que: “Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade nos termos desta Lei.”

E o artigo 18: “O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento mediante requisição: (...)”.

A pergunta é: esse artigo 17 da Lei 6.015 está em vigor da mesma forma que na década de 1970? O que se extrai

desse texto de lei é a mesma coisa? A LGPD não mudou o texto da lei, mas a norma é dinâmica. Nós extraímos a norma do texto da lei conforme o cenário, conforme o momento.

Então, parece que a LGPD vai mitigar isso. Quanto vai mitigar? Essa é a questão que vai causar muito debate, porque a solução vai acabar vindo de jurisprudência, do entendimento de uma Corregedoria.

Qual é o limite, o que podemos exigir para controlar um acesso a determinada informação? A própria Lei 6.015 trazia expressas algumas exceções à publicidade que hoje nem se aplicam mais, como legitimação adotiva e legitimação pelo casamento. Mas os fatos que hoje mais aparecem como mitigação da publicidade, e que a doutrina trabalhou bastante, têm a ver com a questão da pessoa que mudou de nome e gênero. Nos últimos cinco ou dez anos, nós já debatemos como mitigar essa publicidade. Embora não tivesse LGPD, não havia sentido em dar publicidade de uma situação dessas.

Qual seria o limite dessa mitigação? Do que se deve ou não se deve dar certidão dessa maneira tão restrita? Qual é o objeto da publicidade registral imobiliária?

Primeiro vamos falar sobre a especificação do bem. A unidade matricial hoje já permite fazer isso com muita clareza. E depois disso, os direitos de ônus inscritos. Quando falamos sobre direitos de ônus inscritos, também temos que falar sobre quem são os titulares desses direitos, ou os devedores, os credores desses ônus inscritos.

Talvez o objeto real da publicidade seja a situação jurídica atual

Quais são os direitos e ônus inscritos que devem ser objeto de publicidade? É situação jurídica atual do bem, ou era um histórico de negócios e fatos jurídicos inscritos? O registrador imobiliário dá publicidade de um contrato de compra e venda, ou ele dá publicidade da propriedade?

E me parece que a resposta para isso é a situação jurídica, nós damos publicidade da propriedade. Nós registramos um negócio jurídico que é modo para publicar uma situação jurídica de direito real. Então talvez o objeto real da publicidade seja a situação jurídica atual.

A Lei 13.097/2018, LGPD, trouxe, nos artigos 54 e 55, o reforço da confiança na publicidade registral.

Será que o comprador de um imóvel tem que investigar os vícios dos negócios anteriores? Esse não é o tema da nossa palestra aqui, mas a resposta para isso pode ser a chave para essa questão.



Se pudermos dizer que a interpretação correta do Código Civil, nos artigos 1.245 e 1.247, combinados com o art. 54 da Lei 13.097, é de que a situação jurídica publicizada atual fornece confiança ao adquirente de boa-fé, e é prestigiada, então muito em breve vamos poder dar publicidade somente de uma situação jurídica atual. Dizer quem é o proprietário, quais são os titulares de outros ônus, titular de uma hipoteca, de uma alienação fiduciária. E vamos deixar as informações pretéritas simplesmente na conservação do registro para eventuais questionamentos.

O que nos parece é que a tendência futura é essa, de que a publicidade tem que ser da situação jurídica atual. Embora aqui, com um parêntese: teremos que interpretar melhor a questão da oponibilidade, com um trabalho maior sobre essa regra dos artigos 1.245 e 1.247 do Código Civil.

Existem dados pessoais sensíveis que não devem ser objeto de publicidade? Um exemplo clássico de dado pessoal sensível é a mudança de nome e gênero, caso que se enquadraria na LGPD, no que diz respeito à proteção de dados pessoais sensíveis. RG, CPF, endereço, profissão também são dados pessoais, mas talvez mereçam uma proteção não tão grande quanto dados sensíveis.

Será que podem ser excluídas da certidão as averbações que já foram canceladas, e que eventualmente desabonem o titular do direito?

Por exemplo, uma penhora do imóvel em execução de alimentos na década de 1990. A pessoa pagou a execução e não quer mais que isso apareça na matrícula. Não se pode dar certidão de um protesto cancelado. Então por que de uma penhora feita e cancelada é preciso dar publicidade para sempre? É trabalho para quem lê, saber que tinha penhora, e pode ser desconfortável para o proprietário aquela publicidade para o resto da vida. Há que se pensar nisso de alguma forma.

E olha o que a LGPD trouxe no artigo 18, incisos III e IV, sobre os direitos do titular dos dados.

Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: (...)

III - correção de dados incompletos, inexatos ou desatualizados;

IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;

“É adequado permitir a visualização de todas as matrículas de um cartório? Hoje, pode alguém receber certidões de todas as matrículas de um cartório? E a retirada de um grande lote de matrículas sem explicação dos motivos?”

“Correção de dados incompletos, inexatos e desatualizados”. Estaria atualizada uma informação que menciona uma penhora cancelada?

Com base na LGPD, a pessoa pode pedir ao oficial para que não dê publicidade de uma penhora cancelada, porque o dado está desatualizado. Como fazer isso? Vamos abrir uma ficha nova, vamos passar a dar certidão somente conforme resumo, somente das situações ativas?

Direito a saber do acesso aos dados e do tratamento de dados

Outra questão. O titular do direito, pode querer saber do registrador o nome das pessoas que pediram certidão daquele imóvel dele? Hoje não tem isso, mas me parece também que agora ele tem direito a essa informação com base no artigo 18, incisos I e II. Ele tem direito a saber do acesso aos dados, e do tratamento dos dados.

Então ele pode perguntar quem foram as pessoas que tiraram certidão do imóvel dele no último ano? Hoje não tem nem sistema para controlar isso, mas talvez seja algo que tenha que mudar.

Hoje vemos algumas empresas que aparentemente têm pretensão de construir uma base de tudo que existe em relação a bens imóveis e dados constantes no Registro de Imóveis. Talvez querendo construir uma base paralela, talvez permitindo uma consulta por outra fonte.

Por isso o artigo 6º da Lei 13.709/2018, LGPD, dispõe que “as atividades de tratamento de dados pessoais deverão observar a boa-fé” a finalidade, a adequação, a necessidade e outros princípios do tratamento de dados, o que realmente nos indica com clareza que essas pesquisas devem ser entendidas como abusivas.

Hoje, com as máquinas, com os robôs de pesquisa, com a tecnologia de processamento de imagens e de dados cada vez com maior precisão, em um fim de semana é possível tirar milhares de visualizações de matrícula e com base nisso reconstituir uma base de dados, o que

me parece abusivo porque não está de acordo com a finalidade, adequação, necessidade do que é a informação que está no registro público.

Questões para reflexão

Temos algumas questões para reflexão. Seria adequado permitir a busca de patrimônio imobiliário a partir do indicador pessoal, sem prévia justificativa da finalidade e no âmbito de um cartório?

Depois da LGPD, me parece que essa busca que hoje permitimos pelo indicador pessoal é algo que não se coaduna mais com o atual momento de tecnologia.

Outra questão: é adequado permitir a visualização de todas as matrículas de um cartório? Hoje, pode alguém receber certidões de todas as matrículas de um cartório? E a retirada de um grande lote de matrículas sem explicação dos motivos?

O controlador desses dados é o Oficial. É função pública dele esse controle. No momento de tratar, de compartilhar e dar acesso aos dados, ele tem que verificar se a utilização está de acordo com boa-fé, finalidade, necessidade, adequação, todos esses princípios que dizem respeito à situação daqueles dados que estão sob sua guarda.

E aqui eu trago também a situação da conservação, e não formação de uma base paralela nem pública e nem privada. A Lei 6.015/1973, estabelece, no artigo 22, que os livros de registro, bem como as fichas que o substituem, somente sairão do respectivo cartório mediante autorização judicial. E o que antigamente era ficha em papel, hoje é ficha em outro meio. Mas os dados estão lá.

Pode, então, sair um banco de dados, ser transmitido para alguém? A Lei 6.015 já dizia que não. E o artigo 16 da LGPD dispõe que “os dados pessoais serão eliminados após o término de seu tratamento”.

O artigo 23 da LGPD está de acordo com o estabelecido na Lei 11.977, quando fala do registro eletrônico, bem como com a Lei 13.465 quando fala do ONR. Nunca

se falou em construir base paralela fora dos cartórios. Sempre que menciona “permitir acesso”, a lei não fala em transmitir dado nenhum para ninguém.

Então, já estavam na lei, desde 1973 os fundamentos jurídicos para que a informação como um todo não vá para a mão de um terceiro, ainda que da administração pública. A lei vem reiterando isso: em 2009, quando a Lei 11.977 regulou inicialmente o registro eletrônico; depois foi a Lei 13.465/2017; e agora de novo. A lei sempre fala em acesso. Acesso é diferente de compartilhamento, são processos muito diferentes, e nós temos responsabilidade nisso.

Então, a LGPD traz mudanças para nós, registradores? Parece-me que sim. Nós vamos enfrentar um novo paradigma muito em breve. A lei vai entrar em vigor e temos que conseguir criar novos marcos regulatórios em relação à forma de gerir os dados.

Inicialmente, os dados pessoais têm que estar protegidos, rastreáveis e acessíveis. Hoje nós não temos rastreabilidade. A maior parte dos *softwares* que usamos não tem *login* de quem consultou, não sabemos para quem demos uma certidão. Não temos rastreabilidade dos dados; precisamos passar a ter.

As empresas que oferecem *software* vão ter que se adaptar, os dados deverão estar protegidos e acessíveis. E vamos ter que facilitar cada vez mais a publicidade com clareza somente das situações jurídicas que são pertinentes. As tecnologias têm que permitir acesso cada vez mais facilitado à situação jurídica que deve ser publicizada.

Ao mesmo tempo que a lei exige maior rigor no controle e proteção dos dados, exige também maior facilidade e clareza no acesso aos dados que são pertinentes. Isso também é inexorável no ambiente de tecnologia em que vivemos, e é possível.

E numa outra situação, é possível continuar centralizando dados para fins estatísticos? Sim, a lei já deu a solução: somente dados anonimizados podem ser tratados para esse fim.

Em se tratando de centralização – seja ARISP ou ONR – a finalidade vai ser muito pequena: pesquisa, indicadores e estatísticas, uma vez que quando se fala em centralização temos que tratar dados de maneira anonimizada. E de acordo com a lei, o registrador é o controlador dos dados que estão sob sua guarda.





A publicidade jurídico- registral, seu objeto e veículo de sua difusão



As palestras que me antecederam tocaram



JULIANO MARANHÃO
Professor da Faculdade de Direito da Universidade
de São Paulo (USP)

em temas afetos à filosofia, o que me deixa bastante confortável.

A primeira tratou de ontologias, a seguinte abordou o tema da memória e a última abordou a cognoscibilidade. Todos são temas com profunda raiz filosófica e, no final das contas, o direito lida o tempo todo com questões dessa natureza. O jurista, porém, tem o desafio de dar soluções pragmáticas para essas questões, criando condições para a decidibilidade de conflitos que lhe são apresentados.

Essa é, a meu ver, a grande riqueza do direito: como transformar questões filosóficas difíceis – como justiça, livre arbítrio, causalidade, personalidade etc. – em soluções práticas?

A questão de fundo discutida por todos que me antecederam é a hipótese de possível antinomia entre a *publicidade registral* e a *proteção de dados*.

A preocupação imediata é: mas em que medida esse dever de publicidade não contrasta com uma proteção da esfera privada, individual? Essa é a primeira leitura. Daí a necessidade de refletir melhor sobre o significado desses dois conceitos: o que é a publicidade e, em particular, a publicidade registral; e o que é a privacidade e, em particular, qual o bem protegido pela legislação de proteção de dados.

Publicidade na atividade registral: três realidades distintas

É interessante que essa provocação faz com que os registradores e os juristas dedicados ao direito registral passem a repensar um conceito antes tomado como trivial: publicidade, como tornar público. Mas agora o registrador se vê forçado a uma problematização: o que efetivamente significa publicidade na atividade registral?

Vejo esse problema, aproveitando a palestra anterior que tratou de ontologias, como uma questão que nasce de uma relação entre três ontologias distintas, três realidades distintas.

A primeira é a realidade física, onde nós, indivíduos,

temos nossos atributos, em parte atributos naturais e em parte atributos que construímos nas nossas relações sociais. Então, de um lado o indivíduo como realidade física num conjunto de relações com outros indivíduos físicos.

Do outro lado, uma realidade que é informacional. Vou usar um termo do Luciano Floridi, uma infoesfera. Uma espécie de realidade também construída por sistemas de informação, sistemas computacionais, e que passam a ter, num primeiro momento, uma representação dessa realidade física, mas que, em determinado momento, dela se desprende, como um mundo à parte. É essa virtualidade, a infoesfera, o objeto de preocupação da Lei de Proteção de Dados.

Nessa realidade, um indivíduo passa a ter sua identidade traduzida no conjunto de informações ou de relações entre essas informações que a ele se referem. Com a ampliação da importância dessa infoesfera e do seu impacto na vida social, aquela representação individual, aquele conjunto de informações, e de relações de informações, que se refere a um determinado indivíduo passa a ter consequências também na realidade física.

A terceira realidade em jogo é também virtual: a realidade jurídica. É um mundo próprio, no qual também são feitas representações de objetos e representações de indivíduos. O sujeito de direito é uma representação de determinado indivíduo ou de determinada construção conjunta de indivíduos no mundo físico. E essa representação tem uma série de interconexões que é construída a partir de uma série de relações jurídicas entre esses

indivíduos. Com isso essa virtualidade ganha certa independência, o indivíduo é nela reduzido ao “sujeito de direito”, que se traduz em um feixe de relações jurídicas com os demais sujeitos que configuram o mundo jurídico. Obviamente, essa virtualidade jurídica tem uma série de impactos na vida individual dentro dessa realidade física.

Essas três realidades começam a se entrelaçar. Primeiro, com a regulação jurídica da forma pela qual são tratados os dados na construção de identidades no ambiente informacional.

Então, primeiro há a percepção de que a realidade virtual informacional pode provocar impactos no indivíduo físico e, portanto, a necessidade do direito em estabelecer regras que controlem aquele fluxo e processamento de dados que geram informações.

Segundo, no âmbito desse universo jurídico, ou para usar o termo de Kelsen, o mundo do “dever-ser”, há uma série de atos com significados jurídicos dentro dessa prática social chamada “direito” e que veiculam sua configuração.

É justamente aqui o papel fundamental dos registradores: a configuração do mundo jurídico. São os cartórios que, em grande parte, constituem relações jurídicas, constituem elementos de prova válidos no direito e demarcam aquela referência do sujeito de direito, no mundo jurídico, ao indivíduo específico no mundo físico. A outra instituição que cumpre esse papel, de constituir e declarar relações jurídicas, é o Judiciário, porém, em grande parte, em contexto litigioso.

O papel dos cartórios na construção da realidade jurídica

Então, os cartórios e o Judiciário têm essa função de constituir relações jurídicas e conectar esse mundo virtual jurídico com o mundo físico. E a preocupação que surge nos cartórios, naqueles que exercem aquela atividade, é muito legítima e interessante. Os cartórios percebem que no seu papel de construção dessa realidade jurídica são geradas informações. Informações que podem entrar na infoesfera com implicações significativas na esfera individual.

Daí a pergunta: em que medida essas informações irradiadas naturalmente na prática de constituição do universo jurídico podem trazer preocupações quanto à identidade individual construída na infoesfera?

Para lidar com essa questão temos que entender exatamente qual é o papel dos cartórios na construção dessa

realidade jurídica, e de que maneira essa informação pode irradiar. E, então, entender qual é o papel da Lei de Proteção de Dados no controle das informações, que irradiam da atividade pública notarial e registral, no sentido de cumprir determinações ou regras que controlam o fluxo daquelas informações.

O tema é bonito porque leva os cartórios a um esforço de autocompreensão. Perguntar sobre a publicidade, já que essa é uma dimensão tão importante das atividades dos cartórios, significa questionar o fundamento da própria atividade notarial e registral: o que nós fazemos no final das contas, qual é nosso papel e quais são os limites nessa configuração da realidade virtual jurídica?

A teoria de Searle sobre fatos institucionais fornece uma ferramenta importante para refletir sobre essa questão. Searle, principalmente na obra “The Construction of Social Reality”, parte de uma observação interessante, de que existem determinados fatos que têm uma realidade objetiva, reconhecida coletivamente e independente de valorações subjetivas, mas cuja existência vincula-se a uma prática social institucionalizada.

Existe uma diferença muito grande entre esses fatos objetivos de natureza institucional, chamados de “fatos institucionais”, e os chamados “fatos brutos”. Fatos brutos referem-se a fenômenos físicos que podemos descrever independentemente de uma prática social. Por exemplo, a distância da Terra em relação ao sol é um fato bruto.

E existem determinados fatos institucionais como propriedade, casamento, cuja descrição depende de uma crença coletiva construída por meio de uma prática social. O fato de eu estar casado não aponta nenhum atributo físico que possa ser identificado, a não ser a aliança, que é apenas uma sinalização da existência de um outro tipo de fato, um fato institucional, dependente de uma prática social, inclusive de um ritual, reconhecido e dotado de autoridade.

O que o Searle busca fazer é explicar qual a gênese desses fatos institucionais. Ele identifica que os fatos institucionais não são convenções arbitrárias, mas dependem de uma prática social institucionalizada por meio de regras, mas regras que têm uma característica distinta, que ele chama de “regras constitutivas” ou “definitórias”.

Existem regras que regulam ações, as chamadas regras regulativas. Por exemplo, “dirija pela direita”. O comportamento conforme à regra, a ação de dirigir pela direita, existe independentemente da regra. Agora



a prática de mexer uma peça de xadrez, por exemplo, mexer horizontalmente ou verticalmente uma torre, ela só tem significado dentro do jogo de xadrez.

A regra constitutiva define a própria prática, ou seja, aquilo que faz sentido dentro da própria prática. Quando, no direito, indico alguém como proprietário, eu faço um movimento dentro daquele universo de relações jurídicas que só faz sentido dentro da prática institucional que é chamada “direito”.

Eu não entendo alguém como proprietário independentemente dessa prática institucional. Também não entendo alguém como casado, fora das regras constitutivas das condições de validade do casamento. O casamento é um *status* gerado pelo ritual que só tem significado a partir das regras que o constituem e vinculam objetivamente a todos. O direito, portanto, é construído sobre

uma série de fatos institucionais que são determinados por essas regras constitutivas.

Agora, essas regras constitutivas compõem esse mundo jurídico não de forma independente e abstrata. Elas precisam de determinados atos concretos que são chamados “atos performativos”, que instanciam as regras e criam os objetos jurídicos.

E é nesse momento que entra o papel dos cartórios e dos registradores. Quando olho para a finalidade dos registros públicos, qual seja, conferir autenticidade, segurança das relações jurídicas – ou para os atos dos tribunais, de declarar, constituir relações jurídicas – identifico atos performativos que em função de regras constitutivas vinculantes são dotados de autoridade e impõem deveres sobre toda a coletividade, geram crenças objetivas. O fato de que alguém é proprietário,

“Quando falo de proteção de dados não trato propriamente, ou não somente, de segurança do dado ou da informação. Não é o dado que se protege, o que se protege é o indivíduo diante do tratamento computacional de dados.”

um fato objetivo dado por uma crença coletiva, é decorrente de toda essa estrutura de regras constitutivas e determinados entes a qual é atribuída autoridade para realizar atos performativos e assim criar objetos jurídicos. Objetos, porque eles têm uma realidade objetiva. E aquela crença coletiva que recai sobre a autoridade e gera o efeito performativo é o que chamamos no direito registral de “fé pública”.

É disso que estamos falando. Sobre essa base teórica podemos entender e pensar sobre o sentido de publicidade registral.

Entendo, em primeiro lugar, por que faz sentido que essa atividade esteja sob a égide do Poder Judiciário e seja fiscalizada pelo Poder Judiciário. Porque no fundo nós estamos falando de atos performativos que constroem e identificam atos, identificam objetos particulares, concretos, dentro do mundo jurídico, e estabelecem as suas relações.

O que tenho, em cada ato performativo de um cartório ou de um tribunal, é a criação de uma espécie de objeto jurídico, um dado jurídico. O dado jurídico pressupõe determinado juízo por uma autoridade que detenha competência, seja um cartório ou seja um juiz.

E, nesse sentido, essas autoridades constituem ou comprovam relações e *status* jurídicos a sujeitos de direito. Mesmo os atos dos cartórios de natureza chamada “comprobatória” também geram fatos institucionais, porque criam um documento com força probante. O instrumento de prova gerado pelo cartório por meio das certidões é um novo dado na realidade jurídica, um fato institucional. E essa qualidade jurídica do documento tem um significado próprio dentro do universo jurídico, dentro da realidade jurídica.

Publicidade do ato registral: o que é?

Ou seja, dentro dessa construção teórica, o que é essa publicidade do ato registral?

Primeiro temos que separar a produção do dado jurí-

dico, daquele objeto que entra no mundo jurídico por um ato performativo. É esse ato performativo que é público e não a informação.

A informação e os dados manipulados pelos cartórios são dados pessoais e de natureza privada. Sobre eles os cartórios exercem sua função pública. E sua função pública refere-se a uma publicidade jurídica específica que não se confunde com divulgar indiscriminadamente informações.

Ou seja, não se trata da publicidade no sentido de transparência, ativa ou passiva, das atividades da administração. Trata-se de publicidade jurídica, vale dizer, a produção de um efeito jurídico, que confere validade ou eficácia a determinados atos, inscrevendo-os no mundo jurídico. E o que é peculiar desse ato público é que o efeito não ocorre por uma publicação indiscriminada, como no caso de publicação de uma lei, mas por uma disponibilidade concreta por meio de requisição específica.

Então, quando se lavra uma certidão a requerimento de interessado, realiza-se, na verdade, um ato performativo que cria um dado jurídico. Isso é uma atribuição pública de um poder público delegado.

A publicidade é um dos elementos da regra constitutiva que cria dado jurídico por força da atuação do cartório e do notário. Então esse é o sentido primordial de publicidade totalmente distinto da divulgação de informações. Ele existe e se constitui no mundo jurídico não no mundo fático. O cartório, e os registros, e os juízes não comunicam informações. Não é essa a sua atividade essencial. Eles exercem uma competência pública para constituir objetos jurídicos, a partir de dados e informações.

Por isso é também importante separar o que é o conceito de dado daquilo que é informação. Dado, num sentido abstrato, é qualquer marca distintiva, ou qualquer quebra de uniformidade no plano. Pode ser um conjunto de símbolos com tinta numa folha em branco, pode ser uma sequência de *bits* em um sistema computacional.

Isso é um dado. Uma outra coisa é: o sentido, semântico ou pragmático, que se extrai dessas marcas. Essa é a informação. Quando falo que o cartório cria dado jurídico, ele está criando marcas distintivas nessa realidade jurídica. Essa é sua função especificamente jurídica.

É claro que dessas marcas distintivas também se pode extrair significado, significados relevantes que vão entrar na esfera informacional e podem ter implicações importantes.

LGPD e os limites da transmissão de informações

A questão agora é entender, diante da LGPD, quais os limites da transmissão de informações que são reflexas à atividade jurídica registral. Do outro lado também aparece o compartilhamento de informações perante outros órgãos públicos.

Isso faz com que nós tenhamos que entender exatamente o que significa a proteção ou o objeto de proteção da Lei de Proteção de Dados. A nossa preocupação agora está clara: a publicidade tem a ver com o ato performativo que o cartório exerce dentro da sua função pública, no poder que lhe é delegado. Mas ele pode irradiar informações. Como controlar isso? Isso deve ser controlado? A preocupação aqui é de que maneira se pode minimizar essa irradiação de informações.

Com relação a Lei de Proteção de Dados, é fundamental olhar para a decisão judicial que deu origem à proteção de dados, o precedente do Tribunal Constitucional Alemão, no qual foi consagrado o direito fundamental à autodeterminação informacional. Tratava-se da inconstitucionalidade de uma lei de censo que colhia uma série de informações sobre os alemães. A preocupação não era propriamente com o envio de dados, mas a incerteza sobre aquilo que poderia ser extraído da informação a partir da capacidade de processamento computacional dos dados.

Qual o objetivo ou finalidade do processamento e qual seria exatamente a aplicação das informações? A preocupação não está com o sigilo ou reserva, mas com a possibilidade de o indivíduo controlar o emprego da informação.

Na medida em que a informação se refere a mim, eu tenho a prerrogativa de entrar nessa esfera e controlar minha autoapresentação na esfera informacional. No fundo, é uma atribuição de poder para controlar e participar ativamente da construção da autoapresentação de cada um na esfera pública, daí porque o direito à au-

todeterminação informacional deriva não somente da privacidade, mas também do direito ao livre desenvolvimento da personalidade e da liberdade de expressão.

Daí uma dimensão coletiva do direito à proteção de dados, ou da autodeterminação informacional, que tem a ver com a preocupação com uma construção legítima e democrática da esfera pública.

Não estou lidando apenas com a liberdade de expressão como uma particularidade do meu florescimento individual, nem como proteção da minha privacidade individual. Não estou lidando somente com o direito individual. Estou lidando com uma autodeterminação informativa que tem relevância fundamental na construção de uma esfera pública democrática.

Cuidados com a terminologia empregada

É preciso tomar algum cuidado com a terminologia empregada. Quando falo de proteção de dados não trato propriamente, ou não somente, de segurança do dado ou da informação. Não é o dado que se protege, o que se protege é o indivíduo diante do tratamento computacional de dados.

A ameaça não vem tanto do dado, mas tem a ver com a informação que é extraída do dado e cruzada para afetar a autoapresentação individual na esfera pública. A ideia é controlar, ter mecanismos, atribuir poder aos indivíduos para controlar essa autoapresentação por meio de restrições ao processamento dos dados, às informações que são geradas por esses dados.

Outro termo enganoso é o “titular do dado”. Isso porque um dado não é, *per se*, referente ao indivíduo. Posso ter dados que não têm origem num elemento pessoal, mas que pelo cruzamento das informações, apontam para um indivíduo. É quando construo uma identidade informacional, e a atribuo a alguém na realidade física, que o dado se torna pessoal. Por isso prefiro falar não no titular do dado como algo que eu tenho, o que traz associações com propriedade. Melhor falar em um dado que permita uma construção informativa que faça referência a determinado indivíduo. Assim não se trata bem de propriedade, mas de um desdobramento de direitos da personalidade que trazem prerrogativas ao indivíduo quando as informações extraídas dos dados a ele se referem.

Separação informacional de poderes

Um corolário fundamental na construção desse espaço democrático que o poder atribuído pela Lei de Proteção

de Dados dá a cada indivíduo é aquilo que é chamado pelos alemães de separação informacional de poderes. Isso tem a ver com essa preocupação da irradiação de informações que é produzida pelo exercício de competências legais, públicas.

A Administração pode exercer a sua competência e, para tanto, coletar dados e gerar informações. Mas essas informações devem ficar contidas. Os dados que são gerados no exercício dessa atividade têm que ficar contidos dentro daquela esfera específica de competência. É a competência legal que determina a finalidade do processamento e que, portanto, nela se esgota.

Portanto, um corolário do direito à autonomia informacional é que órgãos públicos que exerçam competência no processamento de dados e extração de informações não podem cruzar ou transferir entre si essas informações a não ser quando determinado por lei e com finalidades específicas.

Isso está na raiz da proteção de dados enquanto proteção até perante o Estado. Foi a ameaça de criação de uma unidade informacional e de um poder informacional concentrado nas mãos do Estado que motivou a decisão do Tribunal Constitucional Alemão de 1983. Hoje olhamos mais para a concentração de poder informacional nas mãos das grandes plataformas de internet, mas a preocupação com a circulação de dados e concentração no setor público é fundamental.

E a chave para esse controle, no setor público, está no controle de finalidade a partir da competência ou política pública específica exercida por determinado órgão público ou ente delegado. Como todo controle de direitos nas democracias constitucionais contemporâneas a proteção de dados reside não só na garantia de um direito fundamental, a autodeterminação informacional, como também na separação de poderes.

Dessa ótica não há antinomia entre a atividade registral específica e a proteção de dados pessoais. O tratamento de dados pelos registros é legitimado, pois o sujeito do dado conhece a sua finalidade específica, dado pela competência legal. Não há perda de controle do emprego do dado pessoal ou situação de incerteza que afete sua autodeterminação informativa.

Há uma preocupação em relação àquilo que pode irradiar de informação e que extrapole o exercício da competência específica. Daí a necessidade de revisar como se exerce cada competência registral para conter essa irradiação ao mínimo necessário, o que é um dos parâmetros previstos na LGPD, por exemplo.

LGPD e a legislação sobre dados eletrônicos na Administração Pública

Mas se há alguma antinomia com a LGPD, ela reside em seu confronto com a legislação sobre dados eletrônicos na Administração Pública. Essa legislação extrapola a irradiação dessas informações e gera um descontrole completo dos sujeitos do dado sobre seu emprego.

Quando os decretos do Sinter e Sirc falam da “transferência e gestão da base de dados jurídica”, “base própria constituída por dados registrais”, tratam não de acesso a informações específicas, como preconiza a LGPD, mas da transferência da base de dados produzida pelos cartórios e em relação à qual têm o dever de guarda e conservação.

É sintomático que naqueles decretos se fale genericamente em construir essa base de dados para apoiar a “gestão de políticas públicas”. Isso entra diretamente em confronto com aquilo que determina a LGPD.

A LGPD prevê a possibilidade de fornecer acesso à Administração Pública tendo em vista determinadas finalidades ou políticas públicas, que é uma das hipóteses autorizadoras no tratamento de dados pessoais no artigo 7º, ou seja, poderá ser realizado pela Administração para a execução de políticas públicas previstas em lei.

O parágrafo terceiro estabelece que o tratamento deve considerar “o interesse público” (no singular) que justificou a disponibilização. E também o art. 26 da LGPD dispõe que o uso compartilhado de dados deve atender a finalidades específicas da política pública prevista em lei. De tal forma que uma legislação que obrigue a transferência da base de dados com a indicação genérica de atender finalidades de interesse público não parece cumprir esse comando.

Mais do que isso, frustra completamente a separação informacional de poderes na medida em que permite a livre circulação dos dados entre diferentes ministérios e órgãos públicos sem especificar a finalidade do uso do dado. Gera-se incerteza sobre as informações extraídas dos dados e sobre a finalidade de aplicação e cria-se a ameaça de unidade informacional nas mãos do Estado.

Existe alguma antinomia entre os registros públicos e a proteção de dados? Eu não vejo antinomia de forma alguma no exercício primordial e típico da atividade registral e cartorial, que é a criação daqueles atos performativos que geram dados jurídicos que são fatos institucionais, fatos do mundo jurídico.

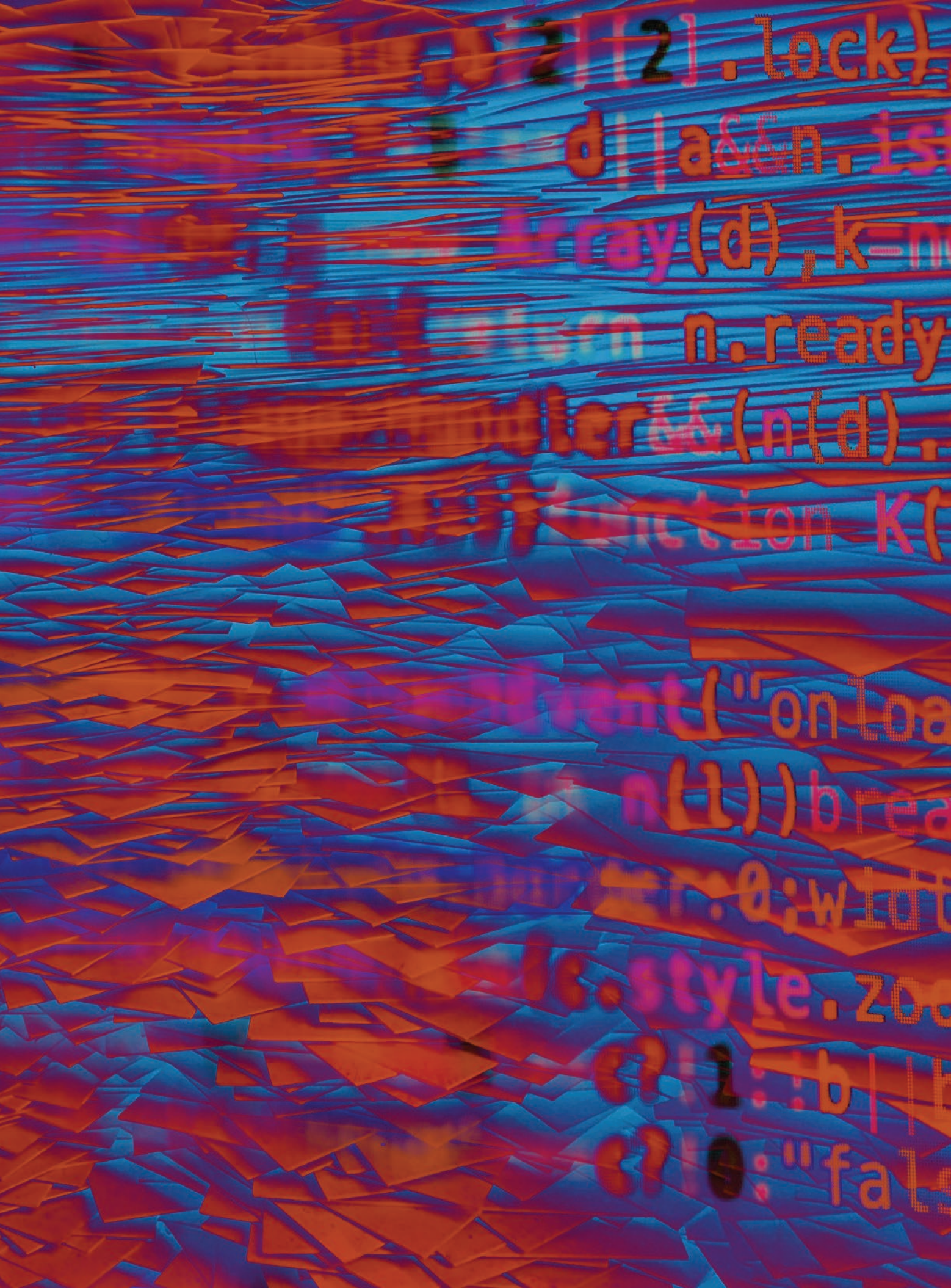
Existe uma preocupação com aquelas informações que podem irradiar. E aqui podemos fazer um exame de

complementaridade entre aquelas regras que se aplicam também ao registro de preservação do sigilo e de conservação daqueles dados no sentido de buscar minimizar a irradiação de informações pessoais. E a Lei de Proteção de Dados traz esses instrumentos.

Eu vejo uma antinomia clara entre a legislação sobre dados eletrônicos na Administração Pública e a Lei de Proteção de Dados. Essa legislação de processamento de dados eletrônicos remete à lei do censo que foi considerada inconstitucional pelo Tribunal Constitucional Alemão em 1983, e foi um marco para o próprio nascimento da proteção de dados como um ramo do direito.

Portanto, a legislação sobre dados eletrônicos na Administração, da forma como está, é um retrocesso em relação à proteção de dados e, por consequência, em relação à construção de uma esfera pública informacional democrática.





Boas práticas e governança no tratamento de dados registrais



No contexto do extrajudicial, sem



CLAUDIO MACHADO
Especialista em Gestão da Identidade do Cidadão e
Planejamento de Tecnologia da Informação

dúvida este seminário será um marco pela profundidade das discussões, a identificação dos desafios, e a oportunidade de tantas pessoas do setor com diferentes perspectivas estarem aqui discutindo e colaborando para o esclarecimento dos impactos da LGPD no dia a dia do extrajudicial.

Um ponto inicial que eu gostaria de enfatizar é que a LGPD não veio para bloquear o processamento ou compartilhamento de dados. Isso não só continuará acontecendo, mas cada vez mais as novas tecnologias, os novos modelos de interação da sociedade, vão exigir o compartilhamento de dados entre organizações e entre pessoas.

A LGPD veio para reger esse compartilhamento e preservar direitos fundamentais das pessoas no meio eletrônico. Eu diria que não existe nenhuma unidade do extrajudicial hoje que trabalhe de forma isolada, que não troque dados com alguma outra organização, seja um cartório, um órgão do Judiciário ou um órgão do Executivo.

Não se trata de proteger os nossos dados, a LGPD veio para reger o uso dos dados, preservando direitos.

Trataremos aqui de aspectos que eu diria que são quase fundamentos ou pré-condições técnicas da implementação da LGPD.

Nós estamos a menos de um ano da entrada em vigor da LGPD.

Como se adaptar à LGPD: orientações básicas

A Gartner, talvez a maior consultoria de tecnologia de informação do mundo, publicou um artigo muito interessante com base na experiência da implantação do regulamento europeu, a GDPR. Nesse artigo, estão sintetizadas cinco orientações de onde se começar para se adaptar à LGPD.

1. Apontar um responsável por proteção de dados. Está na lei, explicitamente, que é necessário ter um responsável pela proteção de dados. Esse é quase que um início de toda adaptação.

Na LGPD esse perfil é do encarregado. Todas as organizações, e no caso do extrajudicial, todos os cartórios e associações representativas, devem ter um encarregado pela proteção de dados pessoais.

2. Realizar um diagnóstico e um plano de ação de adaptação. Avaliar os seus ativos de informação, avaliar os seus processos, fazer um diagnóstico de como você trata os dados na sua organização, como você protege os dados. Quais são os dados que você tem? Você tem dados sensíveis? É necessário realizar essa avaliação de forma estruturada.

3. Definir políticas e rever processos de negócios. Se a prática atual não está em conformidade com a LGPD, será necessário que seja revista.

4. Formalizar governança de programa de proteção de dados. Ou seja, além de um encarregado, é preciso ter um programa definindo claramente políticas em relação à proteção dos dados.

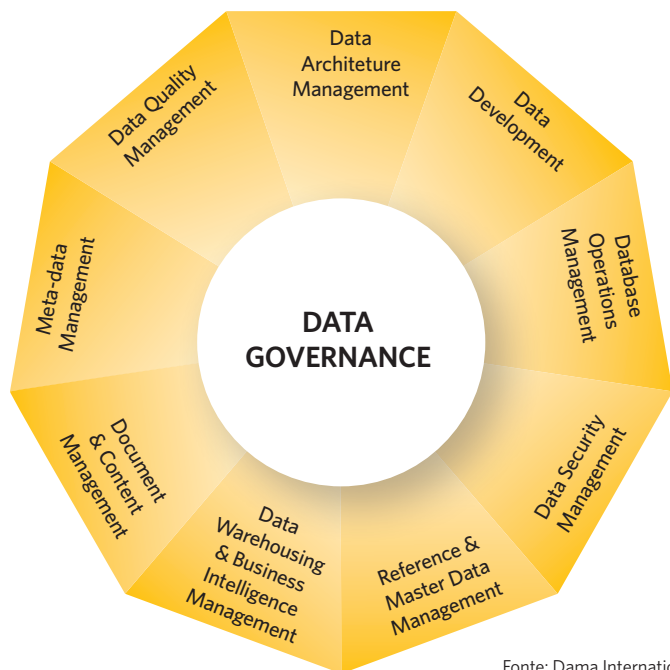
5. Definir um plano de respostas a incidentes. Não vamos nos iludir, incidentes vão acontecer. Toda organização tem problema de incidente de dados, então a prevenção a incidentes é uma exigência. Como reagir? É como a gestão de uma cidade. Você sabe que em determinados períodos vai chover. Precisa ter um plano de prevenção aos eventos.

Implementação da LGPD: governança é a palavra-chave

A reflexão que eu trago parte desses cinco pontos levantados pela Gartner. Toma-se como pressuposto que o entendimento da lei está dado. Não há aqui nenhuma discussão de conceitos jurídicos, são questões relacionadas com a implementação.

O ponto-chave aqui, gira em torno da palavra “governança”. Ela está prevista na LGPD. O artigo 50 trata da questão da governança.

Veamos aqui alguns termos utilizados no artigo 50: “Regras de boas práticas e de governança”; “Condições de organização”; “Regime de funcionamento”; “Procedimentos”; “Normas de segurança”; “Padrões técnicos”;



Fonte: Dama International

“Obrigações específicas para os diversos envolvidos no tratamento”; “Ações educativas”; “Mecanismos internos de supervisão e mitigação de riscos”. Então, é um artigo que sintetiza uma gama enorme de atividades.

Falamos aqui de governança da proteção de dados, ou da governança de dados? Ou das duas coisas?

Estamos claramente diante de um comando para ações de governança de dados, como procedimentos, regime de funcionamento, condições da organização. São atividades internas das organizações que precisam ser aperfeiçoadas para se ter, de fato, uma governança de dados. É um pressuposto para uma ação efetiva de proteção de dados pessoais.

O termo “governança” pode gerar alguma dúvida, então eu trouxe aqui duas visões que se complementam. Uma um pouco mais otimista, que vê a governança como confiança e boa comunicação. É um mecanismo para estabelecer confiança entre os atores envolvidos na organização e obter uma boa comunicação dos objetivos da organização.

E há uma visão um pouco mais técnica, mais dura, que vê a governança como controle e coordenação.

Não se consegue ter uma boa governança sobre aquilo que não se controla. E governança sempre é um mecanismo de coordenação.

É interessante notar que todo mundo é favorável à coordenação, mas ninguém gosta de ser coordenado. Então esse é um dilema que está presente também nesse contexto do extrajudicial. Todo mundo acha que a coordenação entre as entidades é interessante, entre os colegas de um segmento, mas ninguém gosta de perder um pouco que seja da sua autonomia.

Uma definição um pouco mais técnica, voltada para o tema da governança de dados é essa definição da DAMA (Data Management Association). A governança de dados é o exercício da autoridade do controle, planejamento, monitoramento e avaliação sobre a gestão dos ativos de dados da organização.

A DAMA é uma organização internacional independente, de fornecedores de tecnologia ou de serviços de consultoria. É como se fosse o PMI (Project Management Institute) e a ABPMP (Association Of Business Process Management Professionals International) dedicada à definição de boas práticas de governança de dados.

Entre os objetivos da DAMA estão:

1. Preparar as organizações para gerenciar os seus ativos de dados. Quando falamos aqui na LGPD é preciso entender que tratamos de dados não como algo etéreo, mas como um ativo, algo mensurável, algo objetivo que, se não houver métricas, não for documentado, não se consegue gerenciar. E se não se consegue gerenciar, não se consegue proteger. Se não se sabe quem acessa, quem trata, quais são as características daquele dado, se ele foi alterado ou não em algum tratamento, como proteger o dado?

2. Definir, aprovar, comunicar e implementar princípios, políticas, procedimentos, métricas, ferramentas e responsabilidade do gerenciamento de dados. Você passa a ver os dados de outra forma, não mais como um subproduto dos sistemas de informação, mas como um ativo em si, algo que vai ter uma vida independente do suporte em que ele está sendo armazenado e processado. O dado digital tem algumas características diferentes do dado que está no suporte analógico. Aprender a gerenciar esse ativo é um desafio para todos nós não só no extrajudicial, mas em todas as organizações.

3. Monitorar e avaliar a conformidade no uso dos dados. Estamos chegando um pouco mais próximo da LGPD, o uso dos dados. Não podemos achar que basta apenas esse último ponto, o monitoramento do uso. Não vamos conseguir fazer o monitoramento, se não fizermos todo um trabalho preparatório em relação aos dados.

Disciplinas essenciais para governança de dados e adaptação à LGPD

O *framework* de disciplinas da DAMA é amplo, embora não seja pressuposto cumprir todas elas.

Eu vou destacar as quatro disciplinas que na minha

opinião são essenciais para o trabalho relacionado com a governança de dados e adaptação para a LGPD: a segurança dos dados, todas as operações de armazenamento e guarda dos dados, a qualidade dos dados e os metadados.

Vamos pensar nos cartórios. Em qual cartório os dados não estão protegidos? Vamos pensar em dados que ainda estão armazenados em livros. Os livros estão expostos de qualquer maneira? O cidadão, ao fazer uma consulta, tem acesso direto aos livros? Ou apenas uma pessoa com preparação técnica tem acesso aos livros? Existe todo um cuidado relacionado com a segurança e a guarda dos livros. A mesma coisa tem que acontecer em relação aos aspectos digitais.

Sobre o armazenamento de dados, alguns aspectos devem ser considerados. Onde os dados vão estar armazenados?

Como nós estamos? No Brasil tem até uma vedação para se armazenar dados em nuvem fora do Brasil. Portanto, há aspectos relevantes na legislação de armazenamento de dados que precisam ser considerados.

Eu quero enfatizar aqui os aspectos da qualidade do dado e dos metadados. Metadados de sistemas registra-
is. Quem criou aquele dado? Quem acessou? Quem alterou? Qual o formato? Qual o suporte? Metadados são dados sobre os dados. São essenciais para se gerenciar. Se não tivermos metadados sobre os dados, não vamos conseguir gerenciar os dados.

É necessário classificar um dado. E não estamos mais falando apenas dos dados que são capturados pelos sistemas registra-
is. Mas até de dados que talvez hoje sejam considerados acessórios. Quem acessa? Quando acessou? Por qual dispositivo acessou? Qual a localização? São dados essenciais no contexto da proteção de dados pessoais.

Há um diagrama muito interessante que foi objeto de uma tese de doutorado da USP sobre governança de dados¹. Foi a única tese que eu encontrei, o que mostra que o tema ainda é embrionário no Brasil. Ainda não temos uma reflexão acadêmica robusta que testou práticas de organizações brasileiras.

Eu achei muito interessante esse diagrama da autora, porque ela sintetizou o que penso serem os elementos fundamentais para se ter uma governança de dados. Quanto aos princípios, acho que podemos trabalhar com os princípios colocados na própria LGPD.

Além do arcabouço da proteção de dados, há também um princípio adequado para a governança de dados. A



qualidade dos dados, ou seja, métricas que permitam avaliar a qualidade daquele dado. Se aquele dado está íntegro, se está correto.

No meio digital, um problema de qualidade de dados pode criar problemas enormes. Erros sistêmicos podem se propagar de forma a se perder os dados, praticamente. Ao se perder qualidade de um conjunto de dados é possível perder aqueles dados definitivamente.

Além disso, os metadados e ações de acesso aos dados.

Então, acredito que esses são os quatro elementos fundamentais do ponto de vista de práticas para a governança de dados que uma organização deve ter no nosso contexto de implantação dos dados.

ARPEN e a governança relativa à proteção de dados

Fiz uma rápida reflexão sobre como a ARPEN – Associação dos Registradores de Pessoas Naturais está se preparando para a temática da proteção dos dados no que diz respeito à governança.

Então, no que diz respeito à governança, eu diria que um elemento importante foi a criação, pelo Provimento CNJ 74, do Comitê de Gestão de Tecnologia de Informações dos Serviços Extrajudiciais.

O fato é que foi criado um comitê de governança e o próprio provimento limita o alcance do comitê à segurança da informação. Eu acho que é uma coisa, de certo modo, inédita, haver um mecanismo de coordenação de governança de tecnologia da informação no extrajudicial, envolvendo todos os segmentos.

Nós não tínhamos nada parecido com isso. Ainda que seja algo considerado bastante embrionário, e talvez

¹ Furlan, Patrícia. Fatores determinantes para a adoção da governança de dados e de informações no ambiente BIG Data. USP, 2018.

“Pela importância que têm hoje os serviços de compartilhamento de dados, acho que o extrajudicial precisa sim ter mecanismos de governança, de tecnologia e de dados.”

ainda longe de um modelo ideal, mas é uma primeira instância de governança, de discussão de práticas e de políticas voltadas para o extrajudicial.

A própria ARPEN instituiu um comitê gestor para a CRC – Central de Informações do Registro Civil, que é a plataforma da ARPEN para a troca de dados e serviços entre os cartórios e outras entidades públicas.

Esse comitê foi criado no ano passado e tem uma dinâmica muito interessante de discussão. Acho que melhorou bastante a forma de evolução e novas funcionalidades, e de esclarecimento em âmbito nacional da importação dessa CRC, e é um mecanismo de governança.

Foi feito o ajuste dos termos de convênios que já estavam firmados com entidades públicas ou privadas de troca de dados, de acesso a dados da CRC, já pensando na adequação à LGPD. Todos os convênios foram analisados e adaptados, do ponto de vista técnico e jurídico, com os preceitos da LGPD.

Todos os colaboradores envolvidos no tratamento de dados tiveram o contrato de trabalho ajustado para ficar explícito o termo de confidencialidade em relação aos dados – algo que já era um pressuposto, mas tem que estar explícito. Acho que vale a mesma coisa para quem é titular de cartório. Se não estiver no contrato de trabalho de seus funcionários, a recomendação é que não só isso esteja no termo de contrato de trabalho, como também sejam os funcionários orientados em relação às práticas de confidencialidade. Afinal, são eles que vão manipular os dados.

E por fim, está sendo feita uma profunda revisão dos processos de segurança da informação.

Alguns colegas da ARPEN me perguntaram se estamos prontos. Eu respondi que não, tem muita coisa para ser feita, mas isso não é desanimador, porque eu acredito que nenhuma organização no Brasil está plenamente pronta para a LGPD. É um esforço que precisa ser incremental. Nós estamos no terreno da experimentação, não existe uma receita de bolo pronta. A verdade é essa.

As exigências são tantas que, às vezes, dá um pouco

a sensação do mito de Sísifo. Você tem sempre que carregar a pedra até o alto da montanha, ela rola de volta e você começa tudo de novo. Então você pensa: “Eu vou contratar uma ferramenta que vai resolver o meu problema.”

Criar um programa para ficar fazendo esse *looping* não resolve. Não se trata de ferramentas, esse é o ponto. Muitas empresas oferecem ferramentas de adaptação com um *check-list*. Sim, ferramentas são úteis em determinado momento, mas, se não fizermos todo um trabalho preparatório, não adianta. É necessário rever profundamente as práticas relacionadas ao tratamento dos dados.

A Gartner tem um guia passo a passo que é bem interessante. É em relação à governança de dados que eu diria que é mesmo um pressuposto. Se não controlarmos nossos dados, não vamos conseguir protegê-los. Não vamos conseguir cumprir a LGPD, se não tivermos segurança da informação e se não tivermos governança.

Acho que o extrajudicial tem um grande desafio, mas que ainda é um certo tabu. Ele precisa ser enfrentado. Sim, cada cartório, individualmente, tem boas práticas de gestão dos seus dados. Tem responsabilidade com seu acervo, com tratamento daqueles dados. No entanto, quando falamos em tratamento dos dados pelas centrais temos uma interrogação, porque ainda não temos um arcabouço de governança em relação a isso. Não se trata de má-fé. Eu vejo extrema responsabilidade no tratamento dos dados das centrais do extrajudicial. Mas, é fato que não há um regramento estabelecido.

Acho essencial que haja um amadurecimento dessa discussão relativa à proteção de dados. É importante tratar da proteção de dados individuais nas unidades. Mas sem se ter mais clareza em relação a essas novas estruturas compartilhadas de serviços do extrajudicial, eu temo qual será a visão da futura autoridade de proteção de dados em relação às centrais.

Uma coisa é a visão interna, outra coisa é a visão externa. Uma autoridade de proteção de dados vai exigir clareza nos mecanismos de controle, de tomada de decisão, a transparência no uso daqueles dados. Eu escu-

tei muito essa discussão no cafezinho, não aqui. Talvez porque seja de fato um tabu. É um tema que hoje gera algumas discordâncias, mas que não pode ser ignorado. É necessário que esse tema seja tratado com transparência e responsabilidade, pois são mecanismos legítimos.

Algumas questões para reflexão

Eu trouxe algumas questões, que na minha opinião não estão claras do ponto de vista da governança. O extrajudicial não tem orientações no CNJ voltadas para a governança de tecnologia da informação, para a governança de dados.

O extrajudicial deveria adotar os princípios de governança do Judiciário? Ou não, deveria criar seus próprios regramentos em relação à governança por ser um serviço delegado? É uma questão que precisa ser respondida.

Pela importância que têm hoje os serviços de compartilhamento de dados, acho que o extrajudicial precisa sim ter mecanismos de governança, de tecnologia e de dados nesse contexto.

O Provimento CNJ 74 aplica-se às serventias individualmente. O tema é difícil, porque onera o funcionamento de uma unidade, mas, ao mesmo tempo, também é necessária a segurança da informação.

O doutor Antonio Carlos Alves Braga foi de alguma forma visionário, ele disse uma coisa que parece hoje muito longe da realidade. Lembrando as palavras dele: “Olha, eu vejo no futuro um portal em que o cidadão vai lá e para ele não importa se é registro civil, registro de imóveis, ou notas. Ele vai simplesmente pedir o serviço que ele quer e vai ser atendido pela plataforma. E toda a complexidade vai estar abstraída para o cidadão”.

Aqui tem uma previsão interessante: as plataformas do extrajudicial vão estar integradas. Eu concordo com ele. Acredito que isso não esteja tão distante. Vejo como algo que vai ser uma necessidade, uma exigência da sociedade de um país que está se digitalizando de forma rápida.

Quando imaginamos um portal como esse, a complexidade dos procedimentos do extrajudicial terá que ser tratada. Não acho que isso está longe. Se isso não acontecer de forma endógena, as próprias entidades se reunirem e conseguirem criar um mecanismo de autogestão, isso virá de fora. Eu não tenho dúvidas disso.

Acho que a visão do doutor Alves Braga reflete não apenas o pensamento individual dele, mas um anseio de várias autoridades não somente do Judiciário.

Para que tenhamos uma proteção da LGPD segura,

clareza em papéis e responsabilidades, é fundamental as entidades terem domínio técnico sobre o assunto. Acho que não só de tecnologia, e também não só jurídico, mas de gestão em relação a esses temas. O domínio técnico é fundamental, bem como a colaboração entre as especialidades. Isso é imprescindível.

Se não houver colaboração vai ser muito mais difícil essa implantação. Acho que tem que haver ousadia em relação a esse processo. A LGPD não veio para inibir a inovação, ela veio para viabilizar a inovação de forma segura, protegendo os direitos fundamentais do cidadão.

Concluindo minha fala, entendo que o fundamento é que haja clareza e transparência nos mecanismos de compartilhamento de dados. E não se trata apenas de um problema interno, mas de uma questão que envolve também o poder público.

Referências

1. **Provimento CNJ 74** – Dispõe sobre padrões mínimos de tecnologia da informação para a segurança, integridade e disponibilidade de dados para a continuidade da atividade pelos serviços notariais e de registro do Brasil e dá outras providências. Conselho Nacional de Justiça, 2018.
2. **Data management body of knowledge – Versão 2**. DAMA, 2017.
3. **Data Governance: Step-by-Step Guide: Establish the methodology for effective data governance and quality in an era of big data**. Gartner, 2019.
4. Furlan, Patrícia. **Fatores determinantes para a adoção da governança de dados e de informações no ambiente BIG Data**. USP, 2018.
5. Neiva, Cláudio & Willemsen, Bart. **Beyond GDPR: 5 Best Practices for LGPD Compliance**. Gartner, 2019.
6. Ramon Gil-Garcia, J.; Ahmet Gulerc, B.; Pardo, Theresa; Brian Burke, G. **Characterizing the importance of clarity of roles and responsibilities in government inter-organizational collaboration and information sharing initiatives**. CTG Albany, 2019.



Boas práticas e governança no tratamento de dados registrais

7000

3,4,5,6])



A tecnologia foi o principal motivador



ADRIANA JACOTO UNGER
Engenheira (NEAR-POLI-USP)

para a criação da Lei Geral de Proteção de Dados. Sendo assim, vale a pena fazer algumas reflexões sobre o que a tecnologia faz de melhor, que é dar soluções para problemas que não existiam antes.

Isso porque todos os aspectos de segurança responsáveis por manter a integridade, confidencialidade, acessibilidade e disponibilidade das informações já são tratados hoje nas serventias extrajudiciais, para as informações que têm suporte em papel. E já existem procedimentos e processos robustos para manter a segurança dessa informação. Desse modo, o desafio agora é manter o nível de segurança da informação numa outra realidade, que é a dos ecossistemas digitais.

LGPD traz padrões de boas práticas tanto da segurança da informação como da governança dos dados

Vamos tratar um pouco mais sobre o assunto da segurança da informação e tentar aproximá-lo da prática para a adequação à Lei Geral de Proteção de Dados dentro de cada serventia extrajudicial, considerando os tipos de desafios que terão que ser enfrentados no dia a dia.

A própria redação da LGPD é extensa, traz uma série de requisitos e deveres legais a todas as organizações que fazem tratamento de dados, mas não define como isso deve ser implementado. Apesar disso, faz menções importantes sobre requisitos de segurança e padrões de boas práticas, tanto da segurança da informação como da governança dos dados. Destaco os artigos 49 e 50, que tratam explicitamente de regras de boas práticas de governança e da importância de se adotar essas boas práticas. É um convite para identificar, tanto nos padrões nacionais como nos internacionais, quais são essas boas práticas que já tenham sido utilizadas para a segurança da informação e para a governança de dados que possam ser aproveitadas no serviço extrajudicial.

A governança de dados é um assunto muito amplo, que abrange desde a arquitetura de dados. Destaco também a DAMA, que é a associação internacional dedicada especificamente à gestão de dados e que tem um corpo de conhecimento de 10 anos só sobre gestão de dados. Como parte da governança de dados, vamos tratar de uma fatia da governança, o gerenciamento da segurança

de dados, até porque a Lei Geral de Proteção de Dados dá uma importância bastante grande à segurança,

Além do (DMBoK), do corpo de conhecimento para gestão de dados, se considerarmos a ISO e a IEC que são organismos internacionais normativos já com muito mais experiência, representados pela ABNT aqui no Brasil, existe uma família de normas técnicas que é a ISO 27000, que trata especificamente da gestão de segurança da informação. Essa norma tem sido utilizada na própria comunidade europeia por muitas empresas, principalmente do setor financeiro e também em empresas de tecnologia de informação, que desenvolvem soluções de *software*. A ISO 27000 tem sido utilizada por essas empresas como um ponto de partida para se obter adequação à GDPR, que é a regulação europeia de proteção de dados.

Essa família de normas trata a governança da segurança da informação como um sistema de gestão. Desse modo, apesar de ser uma norma técnica voltada para a tecnologia da informação, a ISO 27000 define um conjunto de requisitos de gestão, ou seja, práticas, procedimentos, processos e políticas que têm que ser implementados dentro de cada organização. Nesse sentido, a norma foi projetada para ser aplicável a todos os tipos e tamanhos de organização, organizações públicas, privadas, pequenas ou médias, e pressupõe a implantação de um sistema de gestão de segurança da informação. A implantação da ISO 27000 é muito semelhante à implantação de outras normas de gestão da qualidade, como a ISO 9000 e a ISO 14000. Ela impõe muito mais desafios de gestão até do que controles técnicos propriamente ditos.

Nenhum sistema é 100% seguro: é preciso ter processos internos para a gestão de incidentes

Dentro da família da ISO 27000, a ISO 27001 é a norma que trata especificamente dos requisitos para se implantar um sistema de gestão de segurança da informação. Nessa norma existem 26 requisitos de práticas de gestão que envolvem definição de políticas, responsabilidades,

procedimentos, dentre outros. Existem também, especificados, 114 controles de segurança que são como um gabarito de todas as práticas que devem ser adotadas em termos de *backup*, redundância, gestão de incidentes de segurança, comunicação de incidentes de vazamento de dados, dentre outros. Além de todos esses controles técnicos, há os controles de gestão, que definem quem será responsabilizado, qual o papel de cada um na organização.

A norma tem alguns conceitos interessantes. Em primeiro lugar, a ISO 27000 trata a informação como ativo. A norma subentende que, para se ter um sistema de gestão de segurança da informação, uma das primeiras tarefas a fazer é um inventário de todos os ativos de informação que são tratados dentro da organização. Para cada um desses ativos é necessário também realizar um levantamento das ameaças e vulnerabilidades a que esses ativos de informação estão sujeitos. As vulnerabilidades dizem respeito às práticas internas que, por alguma limitação de recurso ou tecnológica, podem expor a informação a algum nível de risco. A ameaça é em geral uma ação externa que vem se aproveitar da vulnerabilidade para realizar algum tipo de ataque à segurança da informação.

Considerando o sistema de gestão de segurança da informação, a ISO 27000 subentende que não existe nenhum sistema 100% seguro. Ou seja, os incidentes vão acontecer. E, assumindo que vão acontecer, é necessário ter processos internos para fazer a gestão desses incidentes e para ter a continuidade dos serviços quando eles ocorrerem. Tudo isso só é possível a partir desse inventário dos ativos de informação e de um processo de gestão de riscos, incluindo o mapeamento das vulnerabilidades e ameaças.

Não se pode afirmar ou defender que todas as serventias extrajudiciais precisam se certificar pela ISO 27000. Mas apenas como referência, hoje uma empresa de pequeno e médio porte que deseja implantar a ISO 27000 tem que atender a todos os 26 requisitos e todos os 114 controles, ou justificar o porquê de não estar atendendo, num processo de implantação que demora cerca de nove meses. Requer uma transformação interna, definição de papéis, revisão de processos. Não é uma tarefa simples.

“Na prática, está sendo retirada da serventia a tutela do dado e sendo deixado todo o processo, a operação de tratamento do dado.”

E além de todos os requisitos que têm que ser atendidos,

existe, dentro do arcabouço da ISO 27000, também, um processo de governança da segurança da informação. Não basta atender os requisitos, é necessário ter uma direção que define estratégias, políticas, indicadores de segurança de informação, objetivos de não vazamento de dados, de não acesso indevido, é necessário monitorar esses objetivos, esses indicadores, fazer um processo de avaliação que é de melhoria contínua. E além disso, deve existir um processo de garantia que diz respeito à realização de auditorias, tanto auditorias internas como auditorias externas que precisam ser realizadas periodicamente. Deve haver também um processo de comunicação que está bem alinhado com a Lei Geral de Proteção de Dados, que diz respeito à comunicação de incidentes e à relação entre a organização e a autoridade nacional de proteção de dados. Implantar todos esses processos não é tarefa simples.

Dado todo esse panorama, mesmo sem defender que as serventias extrajudiciais tenham que aplicar todos esses requisitos, certamente para o *compliance* com a Lei Geral de Proteção de Dados uma boa parte desses requisitos precisará ser aplicado para manter a segurança da informação dentro de cada serventia. Não se pode deixar de observar uma tendência, que do ponto de vista de segurança é bastante preocupante. Há alguns padrões da teoria de redes em que se tem redes centralizadas, redes descentralizadas e redes distribuídas. A tendência que está sendo imposta nas serventias é que a parte de implantação, de operação, de atendimento aos requisitos de gestão e de infraestrutura está tendendo para a descentralização. Ou seja, hoje, a menos de um ano da entrada em vigor da lei, considerando as dezenas de milhares de serventias extrajudiciais no Brasil, a tendência é que cada uma vá buscar uma solução individual. E essa solução individual será bastante custosa para a gestão, porque além da gestão dos processos no que diz respeito a como são executadas as atividades e à eficiência na prestação dos serviços, é adicionada uma camada da gestão dos dados, ou seja, a gestão da informação, que representa como ocorre o fluxo da informação dentro dos processos de negócios para a prestação dos serviços. As ferramentas serão aliadas nesse processo, mas a gestão terá que ser realizada para que as ferramentas possam responder e fazer o controle de acesso à informação, atendendo todos os requisitos da LGPD.

Na prática, essa pressão por atender mais requisitos de gestão, que é um movimento natural quando a complexidade da operação vai aumentando, está tendendo

“Deixo aqui o SREI como uma inspiração de arquitetura que é capaz de conciliar a descentralização dos dados com o compartilhamento da infraestrutura e dos padrões.”

para a ponta, para a serventia. Isso significa que a operação da serventia tende a ter um custo maior. Por outro lado, outra tendência é a de retirar os dados da ponta e levar para o centro, ou seja, de centralização de dados registrais. Mesmo sem fazer juízo de valor para dizer o que é melhor ou pior, pode-se dizer que, do ponto de vista de segurança, toda vez que se forma uma base centralizada de dados, se introduz uma vulnerabilidade no sistema. Vazamento de dados tem sido uma realidade cada vez mais comum, especialmente nas grandes bases de dados.

Por isso, o sistema atual, por mais que seja hoje predominantemente analógico, sendo um sistema de dados distribuídos, acaba sendo mais seguro do que o sistema centralizado. Na prática, está sendo retirada da serventia a tutela do dado e sendo deixado todo o processo, a operação de tratamento do dado. E, por outro lado, estão sendo adicionados mais requisitos, uma pressão maior de exigências para a operação e para o tratamento de dados na serventia. Essa tendência deve ser observada e ser alvo de reflexão diante dos desafios iminentes, especialmente com o advento da LGPD.

Alternativa: SREI para compartilhar infraestrutura tecnológica e também soluções de gestão

Nesse sentido, não posso deixar de apresentar uma alternativa: a arquitetura do SREI – Sistema de Registro de Imóveis Eletrônico, que está fazendo 10 anos. Quando participei da especificação desse sistema, não se pensava em *blockchain*, mas podem ser identificados mecanismos de garantia de segurança que são semelhantes à da *blockchain*. Não se falava em Lei Geral de Proteção de Dados, mas podem ser identificados mecanismos de *privacy by design*, porque a arquitetura distribui os dados de maneira que o acesso indevido a esses dados acaba sendo dificultado. Então, além de se inspirar nas normas internacionais de boas práticas, de gestão de governança, de gestão de segurança da informação, penso que o SREI também pode ser uma inspiração para se pensar numa arquitetura que possa ser mais segura.

Realizando um estudo com os mais de 100 controles

que estão detalhados na ISO 27000, muitos deles dizem respeito à organização interna de cada empresa. Ou seja, se considerarmos que cada serventia é organizada da forma como o titular decide, esses requisitos são específicos de cada serventia. Cerca de 40% daqueles requisitos, daqueles controles, realmente terão que ter uma solução específica em cada serventia, porque vão depender da organização interna na gestão dos recursos humanos, principalmente.

Entretanto, 60% daqueles requisitos poderiam ser tratados de maneira comum porque, considerando o Registro de Imóveis por exemplo, todas as serventias fazem o mesmo serviço. Para o serviço de Registro Civil, vale o mesmo raciocínio. Se considerarmos os procedimentos e processos, estes poderiam ser também elaborados e compartilhados de maneira uniforme. Se nos inspirarmos na arquitetura do SREI para o compartilhamento da infraestrutura tecnológica, é possível pensar também nesse modelo de compartilhamento de soluções de gestão, principalmente dentro de uma especialidade em que os serviços prestados e os processos são muito semelhantes.

Como conclusão, coloco essa oportunidade para uma adoção compartilhada de boas práticas, e nesse ponto o papel das associações é muito importante para que não fique a cargo de cada serventia ter que implementar todos esses controles de gestão.

Deixo aqui o SREI como uma inspiração de arquitetura que é capaz de conciliar a descentralização dos dados com o compartilhamento da infraestrutura e dos padrões. E também o próprio ONR, que prevê um comitê de normas técnicas justamente com esse objetivo, de promover a integração e a normalização da operação no caso específico do Registro de Imóveis.



**Direito à
informação**

X

**Publicidade
registral**



Minha presença aqui para falar a res



LUÍS PAULO ALIENDE RIBEIRO
Desembargador do Tribunal de Justiça de São Paulo

peito do tema da publicidade e da privacidade, em um espetacular encontro a respeito da Lei Geral de Proteção de Dados, se deve ao fato de que eu me encontro aqui por acidente. Tudo o que me trouxe até este final de evento foram situações nas quais a vida veio me colocando sem prévia programação, de modo “acidental”.

Em 2004 eu era Juiz Auxiliar da Corregedoria, e fui fazer um curso do Cadri na Espanha. Lá tive a primeira oportunidade de conhecer alguma coisa e de ouvir falar algo a respeito da proteção de dados pessoais.

No Brasil, o tema da proteção de dados pessoais era algo que nem se pensava em falar. Vimos alguma coisa lá, e pouco depois caiu na minha mão um livro que eu guardo com muito carinho: *Cuadernos de Derecho Público – Protección de Datos*. Um livro com artigos muito bem escritos relativos à proteção de dados pessoais. Foi muito bom ler tudo isso em 2004/2005.

O IRIB e Associação dos Advogados de São Paulo – AASP promoveram, nos dias 28 e 29 de setembro de 2005, um encontro internacional em São Paulo, voltado à proteção de dados, novas tecnologias e direito à privacidade nos registros públicos.

Nós discutimos esse novo tema nesse evento extremamente interessante. Quem lá esteve participou com muita dedicação. Eu lembro muito bem que ao terminar a minha fala, alguém me perguntou: “Mas os dados que existem no cartório são de quem?” E essa é uma pergunta muito importante quando se vai falar a respeito da proteção dos dados pessoais.

Os dados do cartório são das pessoas que lá depositaram, facultativa ou obrigatoriamente, os seus dados pessoais. Então quando se fala em dados pessoais se está ultrapassando aquela discussão que existia naquela época, quinze anos atrás, a respeito de direito à informação, direito de imprensa, esse tipo de publicidade.

O que foi produzido naquela ocasião? O IRIB colheu o material e o que eu falei foi objeto de um artigo que está publicado na RDI 59, Julho/Dezembro de 2005. É do 4º Encontro – *Publicidade Registral e Direitos da Personalidade*.

Então se começou a discutir, já no âmbito do Registro de Imóveis, o papel do registrador.

Eu sei que vim parar por acidente não só neste evento como naquele em que me caiu na mão um material excepcional, muito bom, a respeito de privacidade, publicidade e proteção de dados. A isso se soma o fato de que, embora eu tenha participado junto com todos da organização deste encontro, eu não estava escalado para falar por último nem junto com o Caleb, que acabou de falar a respeito da certidão, alteração de programa que se mostra providencial. Desde aquela época eu critico a forma de publicidade dos dados dos registros públicos, o que não se mostra adequado.

Naquela oportunidade, já tendo bebido das águas da doutrina e das decisões da Europa, em especial da Espanha, era possível ver que o problema estava chegando ao Brasil. Havia uma situação interessante. Os cartórios ainda viviam uma situação de atomização, em que cada cartório expedia, dava publicidade dos seus atos por meio de certidão, e aqui eu estou falando principalmente do Registro de Imóveis.

Cabia ao registrador, nos termos das Normas da Corregedoria, escolher o tipo de certidão. E a certidão saía por meio dessa escolha que podia ser feita pelo registrador. Em regra, no Registro de Imóveis, se escolhia a certidão por cópia da matrícula, especialmente depois que a matrícula foi instituída, período em que o meio se mostrou eficiente. Mas, já no começo deste nosso século, a certidão por cópia da matrícula parecia algo inadequado. Inadequado por quê? Porque a informação tem que ser suficiente. Não pode ser nem inferior ao necessário e nem abusiva, trazer mais do que precisa.

O Caleb colocou muito bem na sua apresentação que se faz a certidão da matrícula toda. Além daqueles da-

dos solicitados pelo interessado, vão outros dados que deveriam estar protegidos. E conceito de interessado é bem complicado no Brasil, porque nós fizemos uma legislação logo depois de um período ditatorial, e que obriga a fornecer a certidão; o registrador não pode perguntar por quê.

A certidão ainda é o meio pelo qual se dá acesso aos dados dos Registros Públicos?

A publicidade se dava por meio da certidão. Depois desses dois dias de discussão eu pergunto: a certidão ainda é o meio pelo qual alguém interessado – e eu não quero saber que tipo de interessado, se com interesse jurídico ou com interesse não protegido pelo direito – tem acesso aos dados dos Registros Públicos?

Em outras palavras, ainda é a certidão o meio pelo qual se acessam os dados que estão sob a guarda dos registradores? Ou existem outros meios pelos quais esses dados podem vir a ser acessados?

O desenvolvimento tecnológico é algo que muda não a cada dia ou a cada hora, mas a cada minuto. Hoje existem meios e formas de fazer com que informações disponibilizadas de forma livre possam ser apropriadas. Nós temos dois interlocutores que nos assustam no que diz respeito à privacidade e ao serviço registrário. Um é o mercado e outro é a Administração Pública.

Por que o mercado? Porque os dados possuem valor econômico.

Os dados podem ser trabalhados de uma ou outra forma, e eles interessam ao mercado. O mercado pode ser a alavanca de desenvolvimento econômico, mas, esse desenvolvimento não pode se dar com ofensa aos direitos das pessoas, aos direitos à privacidade, à intimidade, aos seus dados sensíveis, e aos dados pessoais que foram confiados ao registrador.

Vamos falar aqui a respeito do registrador imobiliário. Nem sempre o registrador está preparado para fornecer os dados com todos esses cuidados. Quem tem um pouco mais de contato com a atividade percebe que hoje registrador nenhum, ou notário, está preparado para fornecer dados em atenção ao respeito que a privacidade, a intimidade e a proteção de dados pessoais exigem. Por quê? Porque os dados se encontram nos cartórios, todos num formato que não permite ao registrador e ao notário, um corte transversal. Ou seja, os dados ainda se encontram ou em papel ou em fotografias de papel, que é a digitalização, numa situação muito mais próxima do século retrasado do que do século presente.

E só se vai poder cumprir efetivamente a tarefa de dar publicidade registrária, fornecer os dados adequados aos interessados nos negócios imobiliários, aos interessados contratuais, aos institutos de pesquisa, ao poder público, a partir do momento em que os registradores e os tabeliães tiverem esses dados efetivamente trabalhados, desenvolvidos em campos estruturados em que, por meio de filtragem informática, os dados sejam repassados no tamanho certo, nem mais, nem menos. Nem faltando dados, nem com dados excessivos.

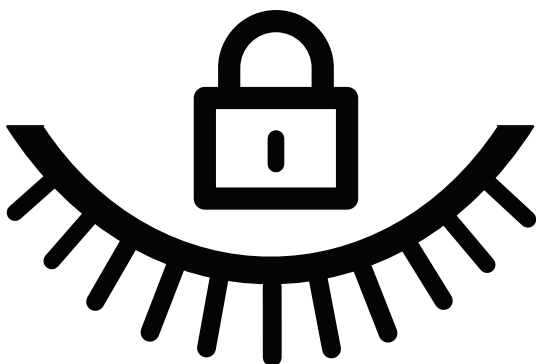
Tratamento de dados pessoais: objetivo é proteger os direitos fundamentais de liberdade e privacidade

E aqui destaco uma coisa interessante. A Lei 13.709, no artigo primeiro, estabelece que essa lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. O artigo 23 dispõe que o tratamento de dados pessoais pelas pessoas jurídicas de direito público deverá ser realizado em atendimento à sua finalidade pública, na persecução do interesse público, com objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público.

E eis a questão: a lei também coloca que os serviços notariais e de registro exercidos em caráter privado, por delegação do poder público, terão o mesmo tratamento dispensado às pessoas jurídicas referidas no artigo, nos termos da lei, e que eles devem fornecer acesso aos dados por meio eletrônico para a Administração Pública, tendo em vista as finalidades de que trata o *caput* do artigo.

Isto posto, destaco que a palavra que mais me interessa e que já me assustara no começo do século – quando fui estudar a proteção de dados na Espanha, e quando estudei aqui no livro mencionado – é “tratamento”.

Nesse livro, Nelson Remolina Angarita, professor da Universidade de Los Andes, na Colômbia, chama de “tratamento”, “qualquer operação ou conjunto de operações efetuadas ou não mediante procedimentos automatizados”. Notem que a redação é antiga, então “automatizados e aplicados a dados pessoais como a obtenção, registro, organização, conservação, elaboração, modificação, extração, consulta, utilização, comunicação, difusão ou qualquer outra forma que facilite o acesso aos mesmos, cotejo ou interconexão, assim como o seu



bloqueio, supressão ou destruição”. Isso é tratamento.

Então, quando se lê que “Esta Lei dispõe sobre o tratamento de dados pessoais” (art. 1º, LGPD) significa pegar os dados pessoais e fazer com eles o que se quiser, para o bem ou para o mal.

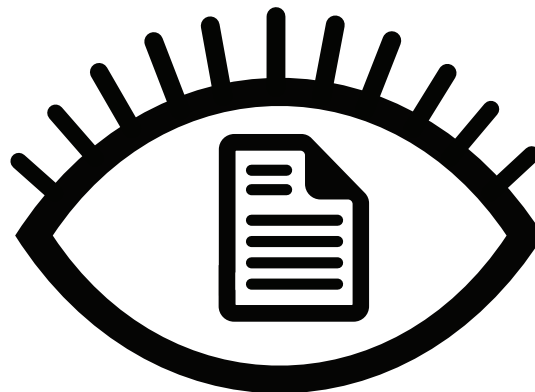
Basicamente, a lei diz que tratamento é “toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração; (art.5º, X, LGPD)”.

O interessado privado não pode receber todo o conjunto de dados de um determinado repositório, de um determinado cartório, de uma determinada especialidade de Notas ou de Registro, porque o tratamento vai ser, com certeza, invasivo e ofensivo à privacidade, à intimidade, e à confiança que a pessoa titular desses dados teve ao depositar tais informações nas mãos do registrador.

Registrador recebe dados que ficam sob sua guarda e aos quais deve dar publicidade para os fins para os quais os dados foram obtidos

Ou seja, os dados podem ser usados somente nos limites e para os fins do consentimento. Os dados foram fornecidos para o uso consentido. O consentimento é fundamental, é o que as diretrizes da União Europeia sempre indicam como algo que tem que ser preservado.

Hoje a riqueza está concentrada nas mãos de quem trabalha com dados, econômicos ou pessoais. Já foi o ti-



tular da propriedade imobiliária, já foi o titular de ações, hoje é o titular de dados que ganha o dinheiro.

É correto arrebatá-los para outros fins os dados dos registros públicos que têm a função de reduzir as assimetrias informativas, de dar informação para que os contratos sejam realizados e que as coisas funcionem? É uma disfunção, é algo errado. Os dados devem ser protegidos para garantia do direito à intimidade, do direito à privacidade, do fundamental direito à proteção dos dados pessoais, corolário até do nosso princípio da dignidade da pessoa humana.

“Interesse público” é uma palavra que, mal utilizada, vira uma coisa demoníaca. Interesse público não é o interesse da Administração, não é o interesse do governo, não é o interesse do leviatã, daqueles que estão ali de plantão assumindo cargos públicos.

Interesse público é uma parcela de cada interesse individual que é, ao mesmo tempo, interesse de todos. Eu tenho interesse. Meus interesses: uns são privados, meus, outros são interesses que cada um de vocês também tem. Nós temos interesses que são de todos em conjunto. Essa parcela do interesse de cada um, que é também interesse de todo mundo, é que corresponde ao verdadeiro interesse público.

É a tutela desse interesse comum que deve ser feita pela Administração Pública, porque esta exerce uma função. E qual é o significado de função?

Função não é só a atividade do cargo público. Não é só a função de Estado: executiva, legislativa ou judiciária. Função tem uma definição muito interessante que me permitiu entender muita coisa. É o sentido que utilizo

“A Administração vem buscando, de alguma forma, a obtenção ilimitada dos dados dos registros e das notas. Será que isso é algo que atende aos direitos das pessoas que ali depositaram os seus dados confiando nos notários e registradores?”

no título da minha tese de doutorado: “Regulação da Função Pública Notarial e de Registro”.

O que é função? Função é a obrigação de buscar, no interesse de outrem, a satisfação de certa finalidade. Qual é a função pública de um tabelião, de um registrador? É atender aos desígnios legislativos para satisfazer um interesse coletivo que não é, necessariamente – e em geral não é – um interesse pessoal desse registrador, desse notário, ou da pessoa que está praticando o ato e que age para dar outros efeitos, efeitos publicitários, efeitos de segurança, a atos e contratos de terceiros.

O notário e o registrador efetivamente cumprem uma função pública. E no cumprimento dessa função pública eles recebem, desses terceiros, dados que ficam sob sua guarda, e aos quais devem dar publicidade – em especial o registrador imobiliário – para os fins para os quais os dados foram obtidos. Mas não além desses fins.

Já naquela oportunidade, em 2005, destaquei, com certa veemência, a questão da apropriação indevida desses dados pelos mercados, pelos titulares do poder econômico. E quando eu escrevi aquilo tudo, trazendo alguma coisa das ideias dos espanhóis, ressaltai que além do valor econômico dos dados eles continuam a pertencer às pessoas titulares desses dados. Usei então a seguinte frase sem que eu ainda tivesse percebido o tamanho da encrenca: “os dados não podem ser apropriados pela Administração Pública para fins diversos daqueles consentidos pelos usuários dos registros públicos”.

A Administração, por meio de um ou outro órgão, vem buscando, de alguma forma, a obtenção ilimitada dos dados dos registros e das notas. Será que isso é algo que atende aos direitos das pessoas que ali depositaram os seus dados confiando nos notários e registradores? Ou, de um certo ponto, confiando na própria Administração Pública e no Estado, porque embora os serviços sejam prestados por exercício privado, eles são realizados por delegação do poder público.

Tratamento dos dados deve conciliar o direito à privacidade e à informação

O tratamento de dados a ser feito deve conciliar tanto a questão da privacidade, quanto da informação.

Eu vejo uma única solução adequada para o futuro dos registros públicos em geral, uma boa transição do meio físico para o meio eletrônico. E transição para o meio eletrônico não é digitalização, não é elaboração de portais para a transmissão de parte das informações ou da totalidade delas.

Passar para o meio eletrônico, efetivamente, significa fazer com que todo o acervo que existe em cada um dos cartórios daqui de São Paulo, ou de qualquer lugar do Brasil, esteja em formato eletrônico, deixando o registrador e o tabelião, preparados para, de imediato, fornecer os dados adequados e necessários. Não é só para expedição de certidão, porque a certidão, hoje, é uma coisa meio inocente, meio inofensiva. O problema é os dados saírem todos de uma vez a partir de sua inserção em meio digital.

É preciso que o guardião dos dados, que me parece que deve continuar a ser esse profissional – o notário, o registrador – possa filtrar e passar os dados adequados para a finalidade daquele que tem interesse em alguma coisa.

A legislação relativa a certidões e a fornecimento de dados também precisa ser atualizada, porque o artigo 17 da Lei dos Registros Públicos, se já era arcaico antes, hoje é temerário, no mínimo.

A questão do interesse, de como demonstrar interesse legítimo é outro ponto importante. A Lei dos registros públicos diz que retardar a certidão é causa de punição disciplinar. E a certidão tem que constar tudo, não se limitando ao que foi efetivamente pedido, ou seja, hoje isso não guarda relação com a realidade.

E se antes a atomização ou a molecularização das unidades de registro protegiam de alguma forma o cidadão, hoje a tecnologia derrubou esses muros todos e fez

com que os dados obtidos de um registrador ou de um notário possam ser trabalhados pelos dois interlocutores: o privado e o público.

Unificação da formalização contratual e da formalização administrativa

E aqui cabe lembrar algo que eu li num livro do Benito Arruñada a respeito de registro imobiliário, dos sistemas de intercâmbio interpessoal. Naquele caso de unificação de informações é preciso pensar muito nos custos e benefícios de se integrar a formalização contratual com a formalização administrativa.

Vamos tentar falar isso em português do Brasil. Os atos e contratos de transferência imobiliária são praticados no âmbito contratual para fins contratuais. Para esse fim os dados são levados a um sistema de registro de imóveis.

A Administração Pública trabalha com esses dados, ou com outros, ou com mais alguns dados, numa formalização administrativa. Deve-se pensar se vale a pena ou não uma tentativa, vamos dizer, estatal, de unificação da formalização contratual e da formalização administrativa.

Hoje nós temos em boa parte do país um bom acervo resultante da formação contratual, são os acervos relativos aos registros e às notas. Esses acervos se encontram numa situação melhor porque foram trabalhados para esse fim. E talvez, a obtenção do dado atual desses acervos possa ser útil, seja para o privado, para o mercado, seja para a Administração Pública, para a formação de cadastros.

O problema é que nós temos que continuar a ter, como alimentadores e atualizadores desses dados, uma entrada, um único *input*. Por quê? Porque esses dados não são estáticos, eles são dinâmicos. Se houve, por exemplo, o risco de duplicação do arquivo, pode acontecer que eu mande meu acervo para um ou outro banco de dados. Eu atualizo o meu acervo, atualizo o seu e não atualizo um terceiro. Esses acervos vão começar a perder aquela fiabilidade que levou a uma tentativa da unificação.

Adverte o professor espanhol: a coexistência de dois tipos de formalização traz dúvidas sobre como eles interagem, porque surgem economias, uma primeira economia, e “deseconomias” – se é que a palavra existe aqui –, quando eles se integram. Então, essas tentativas de unir cadastro e registro devem ser muito bem pensadas.

Estou fugindo um pouco do meu tema, mas é que me parece que a única forma de garantir a continuidade, a fiabilidade dos nossos registros públicos, e que eles não

sejam absorvidos nem pelo mercado nem pela Administração Pública, é criar uma estrutura interna, tecnológica, que permita, a cada registrador ser o guardião efetivo, fiável, dos dados que lhe foram confiados.

Acho que é esse o recado que eu podia dar para vocês com base nos acidentes que aconteceram e no material que veio caindo na minha mão.



LUIZ CARLOS ANDRIGHETTI

**A quarta-feira amanheceu
cinzenta e enevoadada.
Um vento frio movia as
folhas e dobrava os ramos
no quintal. O café tarda,
o trânsito rumora lá fora,
a chuva percute uma
melodia triste no telhado.
Fico sentado, absorto,
afundado num círculo de
pensamentos imperfeitos.
Luiz partiu, a notícia
reverbera em mim.**

Com a sua partida algo essencial se perde, se esfuma e se confunde nas brumas do tempo. Não sei bem o quê – um traço, uma palavra mágica, um nome se extingue, uma luz deita sombras no leito de uma longa estrada, uma estrela se precipita sobre si mesma.

Fico em silêncio. Penso que o Registro de Imóveis, que ele e eu conhecemos há tanto tempo, igualmente se desfigura lentamente. Será o conteúdo e o próprio significado dos pesados livros que de repente se fecham em densos mistérios? Quantas narrativas agora dormem o pesado sono de cifras timbradas pela fé? Ah, Luizinho, a vida anoitece e deita sombras sobre os antigos livros de registro e obscurece nossos corações.

Luiz Andrighetti partiu e com ele se vai uma fração linda e delicada do próprio Registro de Imóveis.

Há um vínculo essencial que me une ao Luiz Andrighetti. Lembro-me de sua caligrafia impecável, de sua perícia inigualável, de sua acuidade, precisão, a capacidade singular de flagrar a pequena nódoa no mar de narrativas titulares. Hoje me ocorre que o seu texto, vazado naquela letrinha caprichada e uniforme, a elegância das capitulares desenhadas com tanto esmero, tudo isso é a expressão humana mais profunda, sublime e delicada que se abre feito uma bela flor dos ofícios. Poucos saberão o significado profundo e sagrado das artes registrais.

Percebo meus pés descalços e frios sobre o assoalho. Desperto de minhas lembranças. Acompanho extático as pequenas gotas que despençam e se arrojam em queda



Luiz Carlos Andrighetti e Miguel Savoy. Escreventes do Registro de Imóveis de São Bernardo do Campo. Foto: SJ, circa 1990.

na janela do quarto. Pequenos meteoros translúcidos, deixam um delicado rastro que se perde e se transforma no percurso. Já são outras gotas que se despedem e assim o ciclo se renova. Assim é a vida, Luizinho, uma eterna dança de transformação e permanência.

Quem viveu o ambiente dos velhos cartórios saberá compreender o que agora lhe confio nesta oração. O vínculo duradouro que nos unia cinzelava os artífices das artes registrais. É o tempo, Luiz, é o tempo que nos aperfeiçoa, que nos lapida, que nos transforma em mestres nas artes de nossa corporação.

Você foi um grande mestre. Nunca cursou uma faculdade de direito, nunca se entretteve com os devaneios e lucubrações acadêmicas, nunca se perdeu no artificialismo de conceitos de moda, nunca, nunca, cedeu à sedução do erro. Você foi um prático, um escrevente que dominava como poucos o saber prudencial, guiava-se por uma espécie de razão prática. Eu sempre o admirei, Luiz, sempre o tive como um exemplo que dignificava a nossa profissão.

Pensando no amigo, não deixo de voltar os meus pensamentos ao próprio Registro de Imóveis, no seio do qual nos desenvolvemos como profissionais e como pessoas. Penso que somos homens de outro tempo, forjados no mister prático, artistas devotados a uma escola de saberes e de conhecimento que nos revela as perenes mutações pessoais e patrimoniais nesta Terra dos Homens. O Registro será uma expressão prefigurada do próprio Livro da Vida, sempre dizia isso, você se lembra?

O que será de nós, Luiz? O que será da Academia do Registro de Imóveis? O que nos sobrevirá e que já se anuncia como nuvens cinzentas no horizonte? Será a tormenta que a tudo arrasa e destrói? Ou a chuva bendita que anima a cepa e fortalece a rama que ainda nos dará um belo fruto?

Não sei Luiz, não sei responder. Sigo seus passos nesta faina diária, guiado pela fé, aquela fé superior que por empréstimo qualifica e dignifica os nossos atos. Sigo na seara cuidando dos brotos e zelando pelo jardim, livrando-o, como posso, da erva daninha e da praga que o assalta na calada da noite.

Luiz nasceu no dia 5 de maio de 1951 em Tupã, interior de São Paulo. Já em 1963 veio com a família a São Paulo e depois de alguns anos estabeleceu-se no Bairro Baeta Neves, em São Bernardo do Campo. Partiria no dia 24 de outubro de 2018, uma quarta-feira. Deixou a esposa, Luziene Gomes Andrighetti e os filhos Rodrigo Gomes Andrighetti e Fernando Gomes Andrighetti

Averbo estas notas como forma de agradecimento à Vida e ao Registro de Imóveis. É esta instituição que me acolheu e formou como profissional e que hoje me permite, na condição de Presidente do IRIB, registrar, talvez como só um velho registrador pudesse, a trajetória deste membro eterno da corporação de ofício dos Registros de Imóveis.

Siga em paz, Luizinho. Sua luz nunca se apagará, querido colega e amigo.

(SJ)

DIRETORIA EXECUTIVA

Presidente: **SÉRGIO JACOMINO** (SP)
Vice-presidente: **JORDAN FABRÍCIO MARTINS** (SC)
Secretário Geral: **JOÃO BAPTISTA GALHARDO** (SP)
1ª Secretária: **FABIANE DE SOUZA RODRIGUES QUINTÃO** (MG)
Tesoureiro Geral: **GEORGE TAKEDA** (SP)
1ª Tesoureira: **DENIZE ALBAN SCHEIBLER** (RS)
Diretora Social: **NAILA DE REZENDE KHURI** (SP)

DIRETORIA NOMINATIVA

Pesquisador de Novas Tecnologias: **CALEB MATHEUS RIBEIRO DE MIRANDA** (SP), Diretor de Relações Institucionais: **DANIEL LAGO RODRIGUES** (SP), Diretor de Tecnologia da Informação: **FLAUZILINO ARAÚJO DOS SANTOS** (SP), Diretor de Relações Internacionais: **IVAN JACOPETTI DO LAGO** (SP), Diretora da Escola Nacional de Registradores – ENR: **DANIELA ROSÁRIO RODRIGUES** (SP), Diretor de Assuntos Agrários: **IZAÍAS GOMES FERRO JUNIOR** (SP), Coordenador Editorial: **IVAN JACOPETTI DO LAGO** (SP)

CONSELHO DELIBERATIVO

Região Norte: **FABIANA FARO DE SOUZA CAMPOS TEIXEIRA** (AC), **JOSÉ MARCELO DE CASTRO LIMA FILHO** (AM), **CLEOMAR CARNEIRO DE MOURA** (PA), **MILTON ALEXANDRE SIGRIST** (RO), **MIRLY RODRIGUES MARTINS** (RR), **MARLENE FERNANDES COSTA** (TO). Suplentes: **RAFAEL CICCONE PINTO** - *In Memoriam* (AC), **FRANCISCO JACINTO OLIVEIRA SOBRINHO** (RO), **KÊNNA ROSALY LOPES TÁVORA** (RR), **IONIZE RODRIGUES DA SILVA** (TO)
Região Nordeste: **JACKSON IVAN PAULA TORRES** (AL), **MILTON BARBOSA DA SILVA** (BA), **ANA TERESA ARAÚJO MELLO FIÚZA** (CE), **FELIPE MADRUGA TRUCCOLO** (MA), **WALTER ULYSSES DE CARVALHO** (PB), **CARLA CARVALHAES VIDAL LOBATO CARMO** (PE), **ABMERVAL GOMES DIAS** (PI), **ALDEMIR VASCONCELOS DE SOUZA JR** (RN), **ESTELITA NUNES DE OLIVEIRA** (SE). Suplentes: **NEUSA MARIA ARIZE PASSOS** (BA), **ANA CAROLINA PEREIRA CABRAL** (CE), **FÁBIO SALOMÃO LEMOS** (MA), **ROBERTO LUCIO PEREIRA** (PE), **SÉRGIO ABI-SÁBER RODRIGUES PEDROSA** (SE)
Região Centro-Oeste: **MANOEL ARISTIDES SOBRINHO** (DF), **ÂNGELO BARBOSA LOVIS** (GO), **HAROLDO CANAVARROS SERRA** (MT), **MARCO AURÉLIO RIBEIRO RAFAEL** (MS). Suplentes: **IGOR FRANÇA GUEDES** (GO), **JUAN PABLO CORREA GOSSWEILER** (MS)
Região Sudeste: **KÊNIA MARA FELIPETTO MALTA VALADARES** (ES), **LUCIANO DIAS BICALHO CAMARGOS** (MG), **EDUARDO PACHECO RIBEIRO DE SOUZA** (RJ), **FLAVIANO GALHARDO** (SP). Suplentes: **JOCŜĂ ARAÚJO MOURA** (ES), **SÉRGIO ÁVILA DORIA MARTINS** (RJ), **JOSÉ CELSO RIBEIRO VILELA DE OLIVEIRA** (MG)
Região Sul: **GABRIEL FERNANDO DO AMARAL** (PR), **CLÁUDIO NUNES GRECCO** (RS), **CHRISTIAN BEURLIN** (SC). Suplentes: **JOSÉ LUIZ GERMANO** (PR), **BIANCA CASTELLAR DE FARIA** (SC), **MARCOS COSTA SALOMÃO** (RS)

CONSELHO FISCAL

Titulares: **GERALDO AUGUSTO ARRUDA NETO** (PR), **MARCELO DE REZENDE C. M. COUTO** (MG), **JÉVERSON LUÍS BOTTEGA** (RS), **AURÉLIO JOAQUIM DA SILVA** (MG), **GUSTAVO FARIA PEREIRA** (GO). Suplentes: **ANDRÉ VILLAVARDE DE ARAÚJO** (PE), **YNARA RAMALHO DANTAS MOTA** (PE), **MARCOS ALBERTO PEREIRA SANTOS** (PA)

CONSELHO DE ÉTICA

Titulares: **ADEMAR FIORANELLI** (SP), **EDUARDO SÓCRATES C. SARMENTO FILHO** (RJ), **MARCOS DE CARVALHO BALBINO** (MG). Suplentes: **ALEXANDRE GOMES DE PINHO** (SP), **SÉRGIO NEUMANN CUPOLILO** (SC), **MIGUEL ANGELO ZANINI ORTALE** (SC)

CONSELHO DELIBERATIVO (membros natos)

ADOLFO OLIVEIRA - *In Memoriam* (RJ), **CARLOS FERNANDO WESTPHALEN SANTOS** - *In Memoriam* (RS), **DIMAS SOUTO PEDROSA** - *In Memoriam* (PE), **ELVINO SILVA FILHO** - *In Memoriam* (SP), **FRANCISCO JOSÉ REZENDE DOS SANTOS** (MG), **HELVÉCIO DUA CASTELLO** (ES), **ÍTALO CONTI JÚNIOR** (PR), **JETHER SOTTANO** (SP), **JOÃO PEDRO LAMANA PAIVA** (RS), **JULIO DE OLIVEIRA CHAGAS NETO** - *In Memoriam* (SP), **LINCOLN BUENO ALVES** (SP), **RICARDO BASTO DA COSTA COELHO** (PR), **SÉRGIO JACOMINO** (SP)



Instituto de Registro
Imobiliário do Brasil

Av. Paulista, 2.073 – Horsa I – Conjuntos 1.201 e 1.202 – CEP 01311-300 – São Paulo – SP.
Telefones: (11) 3289 3599 | 3289 3321 | www.irim.org.br – irib@irim.org.br

Presidente
SÉRGIO JACOMINO
Editora e jornalista responsável
FATIMA RODRIGO (MTb 12576)
Fotos dos Eventos
CARLOS ALBERTO PETELINKAR | kpetelink@gmail.com
Projeto gráfico, diagramação e edição de arte
ELI SUMIDA

ORGANIZAÇÃO



APOIO





Instituto de Registro
Imobiliário do Brasil