

LGPD

Orientações para os sindicatos

Agora está na Constituição!

Constituição Federal:

“Art. 5º. Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

.....

LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.”

LGPD

Orientações para os sindicatos

Título:

LGPD: Orientações para os sindicatos

A Excola desenvolveu este manual, sem fins lucrativos, autorizando seu uso pelas entidades sindicais brasileiras, conforme suas finalidades sindicais, podendo imprimi-la e divulgá-la em seus sites.

Ficam autorizados o download, o upload e a reprodução sem fins lucrativos, desde que mencionada a fonte.

Especificações: cartilha instrutiva, digital, no formato PDF, tamanho A5.

Diagramação: Excola Social.

Imagens e fotografias: Pixabay, de uso gratuito.

Texto: adaptado do prof. Gérson Marques

Nossos agradecimentos ao prof. Carlos Eduardo Pinheiro, advogado no Ceará, pelas lições que inspiraram este pequeno Manual.

Excola Editor.

Fortaleza, Brasil.

Data: junho, 2022.



Caro(a) leitor(a),

A Lei Geral de Proteção de Dados (LGPD) está em vigor e obriga às pessoas jurídicas, de direito público ou privado, a adotar uma série de medidas de proteção aos dados pessoais, em nome dos princípios de privacidade, propriedade e dignidade da pessoa humana.

Tal norma se aplica, também, às entidades sindicais, em todos os graus (sindicatos, federações, confederações e centrais), sujeitando-as às punições previstas em vários de seus dispositivos, o que exige a adoção de providências preventivas. Isso pode, inclusive, exigir a adequação dos estatutos sindicais e a mudança de certas práticas.

Assim, importa que as entidades sindicais a conheçam e a apliquem rigorosamente. E mais: seu conhecimento também deve orientar os sindicatos a atuarem perante as empresas, na defesa dos integrantes de sua categoria. Afinal, o empregador é quem possui os dados mais completos de seus trabalhadores, informações sobre gênero, estado civil, endereço, números de documentos, quanto ganham etc.

Tem, ainda, o campo das relações coletivas de trabalho, onde os instrumentos coletivos podem suprir as lacunas existentes na lei, em benefício de trabalhadores e empregadores.

Portanto, estimamos boa leitura.

Excola Social

Coordenação acadêmica

SUMÁRIO

Introdução	3
Por que compreender a LGPD	4
Do que trata a LGPD?	5
LGPD: uso responsável de dados pessoais.....	5
A LGPD se aplica às entidades sindicais	6
Inaplicabilidade da LGPD	7
Autorização legal para tratamento de dados pessoais	8
O que são “dados pessoais” para a Lei	9
O que são dados sensíveis?	10
Direitos do titular dos dados.....	11
O que é tratamento de dados	12
Requisitos para tratar dados pessoais	13
Como os dados devem ser tratados?	14
Art. 50, LGPD	15
Eliminação de dados	16
Vazamento de dados	17
Princípios previstos na LGPD.....	18
Você já tem um projeto de como tratar os dados no âmbito da sua entidade sindical?	20
Personagens internos exigidos pela LGPD.....	21
O que fazem as autoridades internas	22
O Encarregado: contratação externa ou alguém do quadro.....	23
Sanções previstas na LGPD	25
Responsabilidade solidária	26
CONSIDERAÇÕES TRABALHISTAS DE INTERESSE SINDICAL	27
Estatutos sindicais: adequação à LGPD	28

Os dados nos sindicatos	29
Filiação sindical: um dado sensível	30
O encarregado, na relação de trabalho	31
Obrigação legal trabalhista	32
Decisões automatizadas	33
Legítimo interesse do controlador.....	34
Novas cláusulas coletivas	35
Regulamento Geral de Proteção de Dados (RGPD), na Europa	36

INTRODUÇÃO

Estas orientações abordam as disposições da Lei Geral de Proteção de Dados (Lei nº 13.709/2018), em vigor, que impõe várias obrigações a todos que lidam com dados alheios e estabelece sanções para o caso de descumprimento de suas disposições. Incluem-se aí as entidades sindicais, de todos os graus.

Referida lei tem o propósito de proteger os direitos fundamentais das pessoas, no referente ao tratamento de seus dados pessoais. E isso envolve regras de segurança e transparência da operação, garantindo aos titulares o direito de informação, de alteração dos dados e de encerramento do trabalho. O compartilhamento de dados é permitido, mas dentro de certas regras, que impõem responsabilidades a quem os opera.

Esta regulação não é privilégio do Brasil. De fato, a LGPD vem atender a uma política internacional de tratamento e proteção de dados. Em outros países, há leis semelhantes, até mais evoluídas, como o Regulamento Geral de Proteção de Dados (RGPD, do Parlamento Europeu) e normas semelhantes em diversos países da Europa e das Américas.

Os dados a que se refere a LGPD não são apenas os eletrônicos ou digitais. A Lei alcança, também, o tratamento de dados físicos, aqueles guardados ou arquivados em armários e pastas, como documentos, fotografias, imagens, filmagens, informações obtidas nos currículos dos candidatos a emprego, as fichas de empregados etc.

Sabe-se que os sindicatos obtêm dados pessoais e os armazenam. É o caso da ficha de filiação de associados, que possui várias informações pessoais, como nome completo, CPF, RG, empresa onde o filiado trabalha, filiação, às vezes faixa salarial, endereço residencial, telefone, email etc. Há informações também dos diretores. Na verdade, até as imagens colhidas nas câmeras de segurança são dados pessoais.

Portanto, é preciso compreender a lei para fielmente aplicá-la.

POR QUE COMPREENDER A LGPD

Dois aspectos destacam a importância da Lei para os sindicatos:

- para que a entidade sindical se adeque e, assim, evite as sanções previstas na lei, além de ter de responder por ações judiciais de exibição de documentos e de indenização;
- porque precisará defender seus filiados (ou membros da categoria) perante as empresas que violem a LGPD, ao utilizarem ilicitamente os dados de seus trabalhadores.



Veja a **Lei 13.709/2018** no link abaixo:
(clique sobre ele):

http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

DO QUE TRATA A LGPD?

A Lei nº 13.709/2018 é a **LGPD-Lei Geral de Proteção de Dados**. Ela cuida da maneira como os dados das pessoas podem ser “tratados”, isto é, colhidos, guardados, utilizados e eliminados.

Com esta lei, o Brasil se adequa às exigências internacionais, que já regulam a matéria, e protege as pessoas contra o mal uso de informações a seu respeito. Quando uma empresa, por exemplo, pede o nome e o CPF de uma pessoa ou cliente, certamente fará uso destes dados. Mas, para quê e por quanto tempo? E se a empresa transmitir essas informações a terceiros, o que acontece?

A LGPD não impede que dados pessoais sejam colhidos nem “tratados”. No entanto, ela torna estas operações mais responsáveis, trazendo para dentro da relação jurídica uma série de exigências,

além de estabelecer multas e responsabilidades a quem não observar suas determinações.

O objetivo da Lei nº 13.709/2018 é proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Segundo seu art. 3º, a LGPD é aplicável a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados.

Portanto, também a Administração Pública deve obediência a esta Lei, cujas normas gerais são de **interesse nacional** e devem ser observadas pela União, Estados, Distrito Federal e Municípios.

*LGPD: uso responsável de dados
pessoais*

A LGPD SE APLICA ÀS ENTIDADES SINDICAIS



A LGPD se aplica a todos que lidem com dados alheios, à exceção dos casos que a própria lei relaciona (art. 4º). As entidades sindicais possuem vários dados dos seus filiados e, enquanto empregadoras, também possuem os de seus trabalhadores.

Quais são os dados pessoais com que os sindicatos lidam?

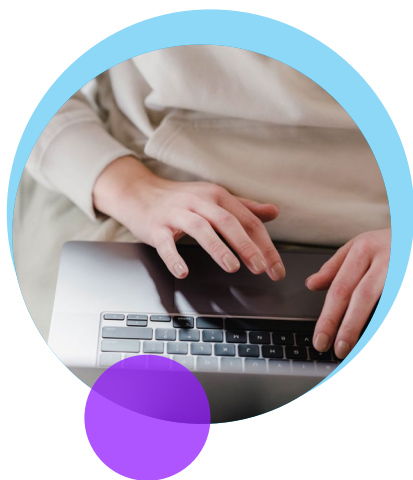
Nomes dos associados, seus CPFs, RGs, endereços, profissões, locais onde trabalham, emails etc. São dados constantes das fichas de filiação. Quanto a seus empregados, a entidade sindical possui estes dados e muitos outros, como o PIS, a CTPS, informações salariais, contra-cheques, filiação, tempo de serviço etc.

Possuem, ainda, informações sobre os diretores sindicais, inclusive alguns dados sensíveis.

E mais: detém documentos, fotografias, vídeos, emails, telefones etc. Pode-se dizer, a grosso modo, que até as câmeras de segurança, internas ou externas, captam imagens, que passam por um processo de tratamento.

INAPLICABILIDADE DA LGPD

As exigências contidas na LGPD não se aplicam nos seguintes casos de tratamento de dados:



(a) realizado por pessoas naturais para finalidades exclusivamente particulares, não econômicas;

(b) realizado para fins exclusivamente:

- ❑ jornalísticos, artísticos e acadêmicos;
- ❑ realizado para fins exclusivos de segurança pública, defesa nacional, segurança do Estado, e atividades de investigação e repressão de infrações penais.

(c) proveniente de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.



AUTORIZAÇÃO LEGAL PARA TRATAMENTO DE DADOS PESSOAIS



Embora a regra seja a exigência de autorização do titular do dado para que haja seu tratamento, há casos em que a legislação dispensa tal consentimento. A autorização legal consiste em (art. 7º da LGPD):

I - consentimento;

II - para o cumprimento de obrigação legal ou regulatória pelo controlador;

III - pela administração pública, quando necessário à execução de políticas públicas previstas em leis e regulamentos ou em contratos, convênios ou instrumentos congêneres;

IV - para a realização de estudos por órgão de pesquisa, garantida, quando possível, a anonimização dos dados pessoais;

V - quando necessário para a execução de contrato ou de

procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral;

VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;

VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais ou órgãos de saúde, ou por autoridade sanitária;

IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular; ou

X - para a proteção do crédito.

O QUE SÃO “DADOS PESSOAIS” PARA A LEI

Os dados pessoais pertencem ao próprio sujeito. Para que outras pessoas os utilizem, dependem de sua permissão, da autorização da lei e da maneira como a legislação determine. Em termos didáticos, pode-se dizer que o titular *cede* seus dados ao controlador para certo tratamento, por tempo determinado ou indeterminado. O princípio é o de que poderá, a qualquer momento, retirar a autorização para o tratamento e desautorizar seu manuseio.

Quando alguém informa seus dados para outrem (ex.: para o sindicato ou para a empresa), não perde sua titularidade. Tanto que pode, a qualquer momento, solicitar informações sobre o seu uso e retirar a autorização de seu tratamento, salvo nos casos previstos em lei.

A LGPD (Lei nº 13.709/2018), classifica os dados em vários tipos. Uma destas classificações é a seguinte:



(a) dado pessoal: é qualquer informação relacionada a pessoa natural identificada ou identificável. Exemplos: informações pessoais (nome, sobrenome, CPF, RG, endereço, filiação, nacionalidade, data de nascimento), fotografias, imagens, cópias de documentos etc.;



(b) dado pessoal sensível: 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.



A Lei se refere, também, aos dados **anonimizados**, que são os relativos ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

O QUE SÃO DADOS SENSÍVEIS?



Além dos dados pessoais ordinários, existem outros que requerem cuidado redobrado, em razão do risco de causar exposições além do razoável e provocar discriminações ou ofender a intimidade da pessoa. Por isso, a lei os tratou de forma especial, limitando seu uso, que só pode ser feito com o consentimento do seu titular ou nas estritas hipóteses previstas em lei.

Segundo a lei, considera-se sensível o *“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, II, LGPD).

O dado sobre **filiação sindical** tem o objetivo de evitar as discriminações sobre os trabalhadores, pelo fato de serem filiados ou exatamente porque não são filiados a nenhuma entidade. Esta previsão é uma das unanimidades nas leis de proteção de dados de outros países.

DIREITOS DO TITULAR DOS DADOS

Os dados constantes dos registros e assentamentos da empresa (ou da entidade sindical) continuam sendo dos seus titulares. Não há transferência de propriedade. Por isso, a LGPD prevê, em seu art. 18, que o titular dos dados pessoais tem direito a obter do controlador, em relação aos seus dados, a qualquer momento e mediante requisição:

- ❑ confirmação da existência de tratamento;
- ❑ acesso facilitado aos próprios dados;
- ❑ correção de dados incompletos, inexatos ou desatualizados;
- ❑ anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
- ❑ portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
- ❑ eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
- ❑ informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
- ❑ informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
- ❑ revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.

Os sindicatos, na defesa de interesses coletivos de seus representados podem fazer denúncias contra os empregadores e agentes de tratamento de dados na ANPD e perante outras autoridades públicas, como o MPT.



Qualquer atividade que envolva a utilização de um dado pessoal na operação de certa atividade é considerada “tratamento”.

Obter ou coletar um dado já integra o tratamento. Processá-lo e compartilhá-lo também faz parte desse tratamento.

O que é TRATAMENTO DE DADOS

Segundo a LGPD (Lei nº 13.709/2018), o tratamento é *“toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração”*.

Portanto, a responsabilidade com os dados inicia-se desde a sua coleta, passando pelo seu armazenamento, por qualquer forma de sua utilização e, por fim, pelo seu descarte ou eliminação.

REQUISITOS PARA TRATAR DADOS PESSOAIS

Em regra, obter dados e processá-los sem autorização do seu titular é ilegal. Compartilhá-los com terceiros é ainda mais sério, pois pode causar exposição e gerar danos civis.

Antes da LGPD, constatava-se que grandes empresas (e até empresas pequenas) se apropriavam de dados de seus clientes ou de seus trabalhadores e negociavam seu compartilhamento sem nenhuma permissão do titular. Esta prática não é mais permitida.

Então, por princípio, o tratamento de dados requer **autorização** do seu titular. Por isso, só com a vontade do titular o dado poderá ser obtido e ser tratado, respeitada a **finalidade** explicitada nas informações transmitidas pelo controlador. A regra, portanto, é pedir as informações e deixar claro para quê os dados serão utilizados.

Certos dados são colhidos por decorrência natural de um contrato, como os nomes dos contratantes, suas identificações, endereços etc.

Em alguns casos, porém, o consentimento é dispensado. Cita-se o tratamento para a proteção à vida, para fins de estudos e pesquisas, exercício regular de direitos e cumprimento de obrigação legal. Exemplo: informações colhidas pelo empregador, por ocasião da admissão do empregado, para alimentação do e-Social. Trata-se de obrigação **legal**.

Quando a lei autoriza o tratamento de dados, dispensando a aquiescência do seu titular, define, de outro lado, sua finalidade. Isto é, o propósito e os limites do tratamento permitido. Então, tais dados não poderão ser utilizados para outras finalidades. Exemplo: os dados obtidos pelo empregador quando da contratação do empregado só podem ser utilizados para fins laborais, especialmente para informar às autoridades e órgãos do trabalho e alimentar sistemas pertinentes (ex.: e-social).

S seja qual for o sistema ou o mecanismo utilizado para tratar os dados pessoais, é necessário estruturá-lo de forma a atender aos seguintes requisitos:

- segurança
- padrões de boas práticas e de governança
- princípios gerais da LGPD e demais normas regulamentares.

COMO OS DADOS DEVEM SER TRATADOS?

O tratamento de dados deve ocorrer dentro de critérios responsáveis e transparentes, é natural que a legislação lance determinadas bases para uma metodologia apropriada.

O vazamento [por definição, *desautorizado*] de dados acarreta responsabilidade da pessoa jurídica e dos sujeitos incumbidos de tratá-los e preservá-los adequadamente. É preciso adotar medidas adequadas de segurança, a fim de evitar o acesso indevido de sistemas e dos arquivos de dados.

Deve-se capacitar os diretores sindicais, principalmente o **Controlador** e o pessoal administrativo, a respeito de seus

deveres e dos cuidados que precisam adotar na entidade sindical, a fim de evitar que cometam atos que possam atrair responsabilidades.

A forma como a política de dados é elaborada e aplicada é objeto de acompanhamento e fiscalização pelo **Encarregado**.

Objetivando evitar a revelação de dados, é imperioso adotar-se medidas de segurança da informação, incluindo, por exemplo, política de tratamento dos dados, procedimentos internos, classificação dos dados conforme sua sensibilidade, controle dos níveis e métodos de acesso, monitoramento permanente do sistema etc.

REGRAS DE BOAS PRÁTICAS E GOVERNANÇA

Ao dispor sobre regras de boas práticas e governança, que precisam ser adotadas pela instituição (empresa, sindicato...), o art. 50 da LGPD determina que elas devem estabelecer:

“condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais”.



ELIMINAÇÃO DE DADOS

A última etapa no tratamento de dados é o seu descarte, a sua eliminação.

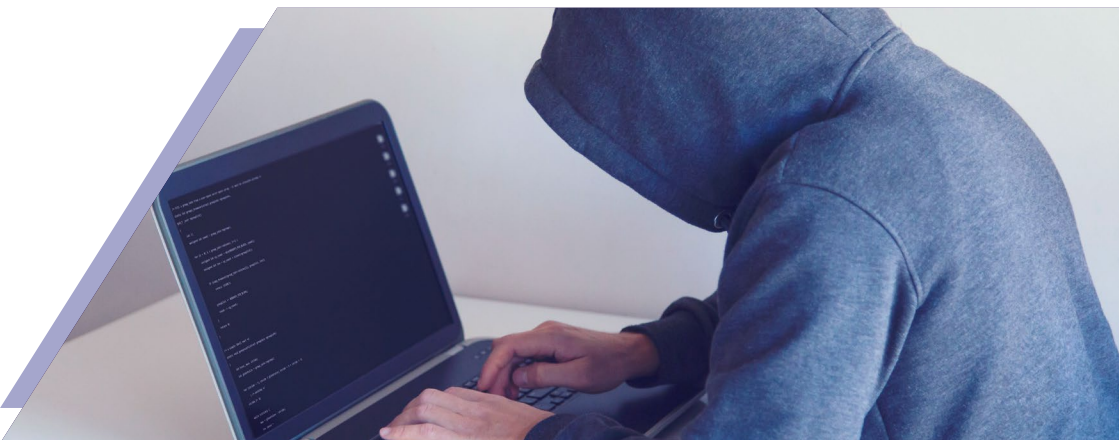
Os dados possuem vida útil, não são entregues para simples armazenamento, exceto nos casos expressamente previstos em lei, a exemplo do controle pelo Poder Público (ex.: órgãos de segurança).

Ao terminar a utilização do dado, ele precisa ser eliminado, o que ocorre quando:

- ❑ tiver sido cumprida a finalidade para a qual fora coletado, quando não for mais necessário ou quando não houver mais pertinência com a finalidade informada;
- ❑ o titular revogar o consentimento (respeitados os casos legais de informação obrigatória) ou se opuser ao tratamento;
- ❑ pelo decurso do prazo de tratamento estabelecido pela organização, conforme determinado pela ANPD-Autoridade Nacional de Proteção de Dados, nos casos de violação à LGPD.

A LGPD prevê, excepcionalmente, a conservação dos dados, mesmo após findo o tratamento, nos casos de:

- ❑ cumprimento de obrigação legal ou regulatória pelo controlador; e
- ❑ para fins de estudo por organismo de pesquisa (ex.: acadêmica), garantida, sempre que possível, a anonimização.



VAZAMENTO DE DADOS

Um dos grandes desafios da modernidade é a proteção contra vazamento de dados, especialmente o ataque de hackers. Grandes corporações têm sofrido com estas invasões. A LGPD se preocupa com esta situação, ao isentar de responsabilidade o controlador dos dados se ele tiver adotado medidas e mecanismos adequados de proteção.

No entanto, o art. 46, LGPD, determina que *“os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de*

tratamento inadequado ou ilícito”.

Determinação semelhante consta do art. 49, ao estabelecer que os sistemas de tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares.

Portanto, se a empresa (ou a entidade sindical, se for o caso) comprovar que o vazamento de dados ocorreu apesar de ela ter adotado todas as determinações da lei e agido conforme as prescrições de proteção e segurança, sobretudo sendo o fato (vazamento) inevitável, então livrará sua responsabilidade (art. 43 da LGPD).

PRINCÍPIOS PREVISTOS NA LGPD

A LGPD estabelece princípios de observância obrigatória. Acompanhe a seguir.

- **finalidade:** realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
- **adequação:** compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
- **necessidade:** limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
- **livre acesso:** garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
- **qualidade dos dados:** garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

O Principal princípio é o da boa-fé, que orienta as condutas de todos os agentes, impedindo pegadinhas, inverdades, armadilhas linguísticas etc.

- **transparência:** garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
- **segurança:** utilização de medidas técnicas e administrativas que protejam os dados pessoais contra acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
- **prevenção:** adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
- **não discriminação:** impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
- **responsabilização e prestação de contas:** demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas. ■



VOCÊ JÁ TEM UM PROJETO DE COMO TRATAR OS DADOS NO ÂMBITO DA SUA ENTIDADE SINDICAL?

É exigência da LGPD a todos quantos lidem com dados alheios que cumpram suas normas e comprovem este cumprimento. Daí, a necessidade do **Relatório de Impacto de Proteção de Dados**, que é um documento no qual deve constar todo o ciclo de vida do tratamento dos dados pessoais e a indicação do fundamento que autoriza este tratamento. Afinal, qualquer manuseio nos dados precisa estar justificado. Este relatório é obrigatório quando o processo de tratamento de dados possa gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

De qualquer forma, mesmo nos casos em que não seja obrigatório o Relatório de Impacto, é importante que haja um **projeto base**, estabelecendo as regras de governança, no qual seja explicitado como se dá o procedimento no tratamento dos dados. Exemplo: a finalidade dos dados coletados, o acesso a eles, sua duração, a quem os titulares poderão procurar, como se dará a atualização e alteração, a maneira de encerramento dos dados etc.

Deve, ainda, por imposição da LGPD, haver fiscalização interna, na própria entidade, independentemente da fiscalização realizada pelas autoridades públicas. Essa fiscalização interna é levada a cabo pelo **Encarregado**.

PERSONAGENS INTERNOS EXIGIDOS PELA LGPD

Internamente, a entidade sindical deve se estruturar de tal forma que se previna contra vazamento ou mal uso de dados, sob pena de responsabilização civil, criminal e sanções administrativas. Por isso, a lei prevê quem são as pessoas incumbidas de lidar com os sistemas e a política de tratamento de dados internamente.

Algumas personagens são previstas em lei, o que exigirá das entidades sindicais considerá-las na sua organização:

- Controlador
- Encarregado



Não se pode esquecer, também, da figura do **operador**, que é o executor das ordens do controlador. É quem realiza, externamente, na prática, o tratamento dos dados, em nome do controlador. Ex.: contador da empresa ou do sindicato, a quem são compartilhados certos dados.



O QUE FAZEM AS AUTORIDADES INTERNAS

Em termos didáticos, o **controlador** é a pessoa física ou jurídica que detém os dados; ao controlador competem as decisões referentes ao tratamento dos dados pessoais. No plano sindical, a entidade sindical é a controladora dos dados.

De sua vez, o **encarregado** (ou DPO-Data Protection Officer) é a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados

(ANPD). Exerce uma atividade de fiscalização interna e funciona, também, como ouvidor dos titulares dos dados, anotando reclamações e podendo sugerir aprimoramentos à política interna de tratamento de dados.

Cabe à entidade sindical tornar público o nome e os contatos do seu DPO (encarregado), informações estas que podem ser divulgadas no site ou página eletrônica do sindicato. E o encarregado, de sua vez, deve estar disponível para reclamações.



O ENCARREGADO: CONTRATAÇÃO EXTERNA OU ALGUÉM DO QUADRO

O encarregado é figura obrigatória, exceto se a ANPD dispensar.

No âmbito **sindical**, é possível que várias entidades contratem um **encarregado** (DPO) comum a todas, o que poderá reduzir custos. Nada impede, aliás, que o encarregado seja um empregado da entidade ou um de seus diretores.

Não é obrigatório ser advogado nem técnico em informática, mas é recomendável alguém com conhecimento da legislação pertinente e que entenda sobre o funcionamento tecnológico do sistema.

O DPO precisa ter certo nível de autonomia para bem desenvolver sua atividade, como acontece com os membros da CIPA.

Empresas estão surgindo no mercado oferecendo serviços de DPO. Ao contratá-las, é preciso adverti-las das peculiaridades sindicais e das prerrogativas constitucionais. A legislação atual ainda não exige uma certificação profissional, embora a tendência seja da exigência de conhecimento técnico. Mas, no âmbito do Poder Público, a Administração já vem exigindo a capacitação do servidor que desempenhar esta função.

Para refletir:

Se um filiado telefonar para o sindicato pedindo informações sobre seus dados, como o sindicato reagirá? Quem o atenderá? Existe algum procedimento para esta ocorrência? E se o titular pedir retificação?



Autoridade Nacional de Proteção de Dados

No CNPDPP, há 02 representantes do setor laboral e 02 do patronal, nomeados pelo Presidente da República, para mandato de 02 anos.

ANPD: Autoridade Nacional

A Lei prevê um sistema de regulação, fiscalização e aplicação de suas disposições, inclusive autoridades encarregadas de sancionar os infratores, como é o caso da Autoridade Nacional de Proteção de Dados (ANPD), a quem o controlador e o encarregado possuem o dever de informação de ofício e sempre que solicitados.

A ANPD é órgão colegiado pertencente à administração pública federal, integrante da Presidência da República (art. 55-A, Lei nº 13.709/2018). Entre seus integrantes estão o Conselho Diretor e o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPDPP).

CNPDPP: Conselho Nacional

O CNPDPP é composto de 23 membros, com atribuição de sugerir ações para a política de preservação de dados, elaborar relatórios anuais, propor diretrizes estratégicas etc.

SANÇÕES PREVISTAS NA LGPD

O art. 42 da LGPD estabelece as sanções administrativas a quem descumprir esta lei. Uma delas é a *“multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R\$ 50.000.000,00 (cinquenta milhões de reais) por infração”*. O valor da multa será destinado ao Fundo de Defesa de Direitos Difusos (Lei nº 7.347/85).

Compete à Autoridade Nacional de Proteção Dados regulamentar o processo de aplicação das sanções administrativas, assegurando o amplo direito de defesa e os recursos cabíveis.

Estas sanções administrativas não excluem as de natureza penal, reparações civis nem outras igualmente administrativas previstas em lei própria, como as referentes aos direitos dos consumidores.

A lei também prevê:



suspensão do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;



suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período.

Banco de emails

Exemplo de punição: suspensão do banco de emails. Isso traria um prejuízo imenso na comunicação da empresa ou do sindicato.

RESPONSABILIDADE SOLIDÁRIA

Uma infringência às regras sobre tratamento adequado de dados pode acarretar sanções administrativas, criminais e reparações civis.

A LGPD possui vários dispositivos a respeito das responsabilidades dos agentes de tratamento de dados, inclusive as indenizações cabíveis em ações individuais ou coletivas.

Vale destacar o teor do art. 42, segundo o qual “o controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo”.

Em seguida, o mesmo dispositivo atribui **responsabilidade solidária** do Operador “quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador”.

E “os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei”.

Se, por um lado, os sindicatos e seus agentes de tratamento de dados podem ser responsabilizados se não cumprirem a lei, por outro poderão questionar judicial e administrativamente atos de empresas que descumpram os princípios e as regras sobre tratamento de dados dos trabalhadores da respectiva categoria.

Como os documentos e os dados se encontram na posse do empregador, é possível o ajuizamento prévio de ações de exibição de documentos ou de pedidos liminares na própria ação principal.

CONSIDERAÇÕES TRABALHISTAS DE INTERESSE SINDICAL

ESTATUTOS SINDICAIS: ADEQUAÇÃO À LGPD



A Lei nº 13.709/2018 não se aprofundou nos seus efeitos trabalhistas nem na abordagem sindical, no que se distanciou da legislação europeia sobre o tema. Então, fica uma margem de subjetividade para que as entidades sindicais verifiquem a melhor forma de aplicá-la e interpretá-la de acordo com os direitos sociais previstos na Constituição Federal, sem abrir mão de suas prerrogativas de representação da categoria. Mas, obviamente, terão de aplicar a lei.

Convém, portanto, que os estatutos sindicais sejam adequados ou alterados para contemplar a previsão de regras gerais sobre tratamento de dados e, principalmente, sobre os **responsáveis** por sua aplicação, como, por exemplo, se o Encarregado será integrante da diretoria, quais suas atribuições, seu mandato, forma de designação ou eleição, se será remunerado, suplência, consequências por mau desempenho etc.

Os estatutos podem, também, deixar que estas designações ou contratações sejam feitas pelas diretorias ou Presidente da entidade. Mais uma competência, portanto, a constar dos estatutos!

Outro ponto importante a constar dos estatutos, até para tranquilizar os filiados sobre como seus dados serão utilizados, é a previsão de regras mínimas sobre o tratamento adequado e a possibilidade de **compartilhamento** dos dados conforme a finalidade sindical, inclusive perante outras entidades de grau superior e chapas em períodos eleitorais. Previsão deste jaez torna todos os filiados automaticamente vinculados à forma prevista no estatuto. No **formulário de filiação**, é possível colher algumas autorizações de tratamento de dados.



OS DADOS NOS SINDICATOS

Segundo a LGPD, os titulares dos dados têm direito à informação clara e precisa sobre como seus dados serão utilizados e tratados. Em outras palavras: ao ceder seus dados à entidade sindical (ou ao empregador), as pessoas precisam estar inteiradas daquilo que será feito com tais informações.

Então, se houver, por exemplo, a necessidade de compartilhamento de dados com terceiros (ex.: centrais sindicais, empresas de seguro de vida, empresas de planos de saúde), convém que a entidade sindical obtenha o consentimento dos trabalhadores. Este consentimento é pessoal, razão pela qual não vale sua obtenção genérica em assembleia. Esta autorização, por outro lado, pode constar das fichas de filiação

ou estar contida no estatuto sindical, conforme mencionado há pouco. Para os não filiados, a autorização deverá ser obtida individualmente, por mecanismos transparentes e seguros da manifestação de vontade.

A LGPD prevê ainda que o titular de dados tem direito à correção de dados incompletos, inexatos e desatualizados, bem como a remoção imediata dos seus dados da base da empresa. Exemplo: Uma pessoa que era solteira e casou, por exemplo, pode solicitar que seja feita a correção do estado civil ou do nome em seu cadastro. Daí a importância de haver canal de comunicação eficaz no âmbito sindical.

Para refletir:

Em eleições sindicais, como os dados serão tratados? As chapas podem ter acesso aos dados dos eleitores? Se for uma eleição eletrônica ou digital, em que os dados serão entregues à empresa que realizará o pleito, como os dados serão compartilhados? Por quanto tempo? Note bem: Se a empresa fizer mau uso dos dados, o sindicato também será responsabilizado.

FILIAÇÃO SINDICAL: UM DADO SENSÍVEL

Os dados sensíveis recebem regulação especial pela Lei. É preciso cuidados redobrados com eles.



Existem dados considerados sensíveis pela Lei nº 13.709/2018, o que implicará na forma como serão tratados. De fato, segundo a LGPD, constitui dado pessoal sensível (art. 5º, II): *“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”*.

Por certo, a empresa precisará ter em seus registros a informação de quais trabalhadores são sindicalizados, para fins de realizar descontos sindicais e outros benefícios obtidos pela entidade. Contudo, esta informação não pode ser utilizada para propósitos sem pertinência com os fins sindicais. A **conduta antissindical** pode se manifestar, por exemplo, se a empresa utilizar esta informação para fins de

discriminação no emprego ou para coagir os filiados a se desfilarem ou os não filiados a se filiar.

E quanto aos diretores sindicais, especialmente os afastados para exercício do mandato, a empresa possui quais anotações? Há algo a retificar? O acesso ao sindicato deve ser garantido, a fim de se inteirar de registros contrários à liberdade sindical. No mínimo, o sindicato interessado deverá ter acesso a critérios, a metodologias e fórmulas de tratamento desses dados, mesmo que sob forma anonimizada.

Considerando que a legislação brasileira é pobre em dispor sobre conduta antissindical e suas consequências, a LGPD pode auxiliar na parte em que estabelece sanções administrativas e ao abrir margem para a aplicação concomitante de sanções civis (ex.: indenizações, reparações), conforme se percebe de seu art. 52, § 2º.

O ENCARREGADO, NA RELAÇÃO DE TRABALHO

Foi visto que o encarregado é figura obrigatória. Então, é importante que os sindicatos atentem à sua condição na empresa.

Pois bem. O empregador terá um **encarregado** de tratamento de dados, como impõe a lei. Se não tiver, estará infringindo a LGPD. Por conveniências administrativas, é possível que o empregador atribua funções de encarregado a algum empregado seu. Caso isto aconteça, o fato deve ficar muito claro no contrato de trabalho e nos assentamentos do empregado, a fim de evitar o desvio de função. Afinal, esta atribuição pode constar no ato de admissão ou ser conferida durante a relação de trabalho. São duas situações distintas, que geram efeitos distintos.

Outro esclarecimento necessário é se o acréscimo de atribuição implicará em alguma **gratificação** e se o desempenho das tarefas ocorrerão dentro da **jornada**

contratada ou envolverá atividades fora do expediente, talvez até fora da empresa. São temas muito adequados, aliás, para negociação coletiva de trabalho.

Foi dito, também, que o **encarregado** deve gozar de certa autonomia perante a empresa, a fim de desempenhar apropriadamente sua função fiscalizatória. Quando se tem relação de trabalho, em que há subordinação jurídica e, não raramente, dependência econômica, psicológica, a legislação costuma atribuir garantias, como **estabilidade** (ex.: cipeiro, representante no local de trabalho). Todavia, a lacunosa LGPD não possui uma única disposição sobre isso. Logo, os instrumentos coletivos de trabalho podem (e devem) tratar da matéria, até porque o trabalho do encarregado, se sofrer interferências do empregador, pode fugir da finalidade objetivada pela LGPD, causando alguma sanção à empresa.

OBRIGAÇÃO LEGAL TRABALHISTA

As empresas devem ter certos cuidados com os dados de seus empregados, não só dos consumidores. É claro que algumas informações são decorrências da legislação trabalhista, porque as empresas precisam delas para cadastrar no e-Social. E, sendo **obrigação legal**, não precisam do consentimento dos trabalhadores para esta atividade.

Contudo, os dados colhidos e armazenados para o e-Social só podem ser utilizados para esta finalidade. Aliás, todos os dados colhidos por permissão da lei trabalhista só poderão ser utilizados para este estrito propósito.

As empresas possuem os dados mais completos dos trabalhadores, como nomes, sobrenomes, apelidos, estado civil, sexo, idade, endereço, telefone, email, filiação, CPF, RG, CTPS, PIS, folha corrida, salário, pensão alimentícia, filhos etc. Praticamente tudo sobre seus empregados.

Muitas destas informações são obtidas ainda na fase de contratação, quando os interessados apresentam seus currículos. Mas... e os **currículos** dos não contratados serão devolvidos, descartados, ou serão digitalizados,

armazenados? A finalidade era, apenas, a candidatura ao emprego! Passada esta etapa, os currículos não poderão mais ser utilizados. Devem as empresas finalizá-los. A não ser que solicitem autorização dos seus titulares, quem sabe para cadastro para uma futura vaga de emprego.

Pois bem. Os **sindicatos** possuem o direito de saber quais procedimentos as empresas estão adotando quanto a estes dados e ter acesso ao **relatório de impacto de proteção de dados**, ao menos na parte referente aos trabalhadores, um documento que se torna exigível das empresas, quando o processo de tratamento de dados possa gerar riscos às liberdades civis e aos direitos fundamentais, ou medidas, salvaguardas e mecanismos de mitigação de risco (arts. 4º, § 3º, e 38, LGPD). Para evitar futura judicialização, estes acessos podem constar de norma coletiva.

E cada trabalhador tem o direito de saber como o seu empregador está tratando seus dados, se não está compartilhando com terceiros, se eles estão corretos e se não estão servindo para fins discriminatórios, o que pode acontecer com o mal uso do dado sobre a cor e a raça.

DECISÕES AUTOMATIZADAS

Rápidas, objetivas e práticas. Mais um campo propício a discriminações.

As decisões tomadas unicamente por tratamento automatizado podem gerar, na prática, desigualdades e irrealidades, o que depende dos algoritmos e da maneira como os critérios de avaliação tenham sido alimentados no sistema.

Por exemplo, avaliações automáticas com base nos índices de produtividade e nos indicadores de integração do empregado na empresa, para efeitos de promoções ou como requisito para manutenção do emprego, feitas unicamente por sistema informatizado, podem ser questionadas. Decisões automatizadas também podem ocorrer na seleção de trabalhadores e para traçar o perfil profissional de empregados.

Afinal, quais são estes critérios ou parâmetros? Que padrões compõem o algoritmo?

O sindicato tem o direito de conhecê-los, desde que demonstre sua necessidade e pertinência para a defesa dos representados.

LGPD

“Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

§ 1º. O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.

§ 2º. Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.”



LEGÍTIMO INTERESSE DO CONTROLADOR

A Lei nº 13.709/2018 possibilita que o controlador trate de dados pessoais para finalidades legítimas (art. 10). O conceito de legítimo interesse é dotado de grande margem de subjetividade, a qual é verificável em situações concretas, considerando, entre outros casos:

I - apoio e promoção de atividades do controlador; e

II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.

Há legítimo interesse quando o tratamento se destinar a: (1) proteção de direitos do titular dos dados; (2) apoio e promoção de suas atividades essenciais; (3) prestação de serviços que gerem vantagens ao titular dos dados; (4) coleta de informações para identificar ou prevenir fraudes; (5) oferta de *marketing* direto; (6) processamento de dados pessoais para análise de perfil de consumidores; (7) elaboração de pesquisas com trabalhadores para criar políticas de bem-estar dentro da organização.

Alguns dados dos trabalhadores podem ser tratados sob o argumento do legítimo interesse, como a coleta de informações que possam fomentar política de benefícios em seu favor. Os sindicatos precisam tomar conhecimento deste fato e analisar se o interesse é, de fato, legítimo.

NOVAS CLÁUSULAS COLETIVAS



Como dito anteriormente, a LGPD não tratou propriamente de assuntos trabalhistas. Muito menos de Direito Coletivo de Trabalho. Há muitas lacunas, portanto, a ser colmatadas. E isso pode ser feito nas negociações coletivas, em acordos e convenções coletivas, de forma a aprimorar a lei e aumentar seu campo de proteção aos dados dos trabalhadores. Veja alguns exemplos próprios de cláusulas normativas:

- ❑ regulação do encarregado-empregado;
- ❑ acordos de interação de dados ou compartilhamentos recíprocos (ex.: relação de filiados, cruzando informações sindicato-empresas);
- ❑ pactos de acesso a metodologias no tratamento de dados de trabalhadores, possibilitando a compreensão de parametrizações;
- ❑ acordos sobre tratamento de dados nas pequenas e médias empresas;
- ❑ troca de dados sobre doenças no trabalho, assegurado o anonimato;
- ❑ maneiras sobre a obtenção de informações quanto à política de tratamento de dados;
- ❑ tratamento de documento sobre antecedentes criminais;
- ❑ regulação de decisões automatizadas e perfil profissional;
- ❑ utilização de equipamento de monitoramento de produtividade;
- ❑ cláusulas sobre compliance trabalhista;
- ❑ regulação do teletrabalho, que inclui a intimidade do lar;
- ❑ criação de mesas de negociação específicas sobre o tema “tratamento e proteção de dados pessoais dos trabalhadores”.

REGULAMENTO GERAL DE PROTEÇÃO DE DADOS (RGPD), NA EUROPA

*Regulamento 679, de 2016, do
Parlamento Europeu (União Europeia)*

Art. 88, I:

“O direito do Estado-Membro ou as convenções coletivas (incluindo «acordos setoriais») podem prever regras específicas para o tratamento de dados pessoais dos trabalhadores no contexto laboral, nomeadamente no que respeita às condições em que os dados pessoais podem ser tratados no contexto laboral, com base no consentimento do assalariado, para efeitos de recrutamento, execução do contrato de trabalho, incluindo o cumprimento das obrigações previstas por lei ou por convenções coletivas, de gestão, planeamento e organização do trabalho, de igualdade e diversidade no trabalho, de saúde e segurança no trabalho, e para efeitos de exercício e gozo, individual ou coletivo, dos direitos e benefícios relacionados com o emprego, bem como para efeitos de cessação da relação de trabalho.”

Segundo o art. 8º, CLT, o Direito Comparado é fonte do Direito do Trabalho. Portanto, a experiência internacional pode orientar a interpretação de casos jurídicos no Brasil.



Conheça os cursos da Excola

- LGPD para sindicatos
- Organização sindical: estrutura e desafios
- Comunicação com a base e os filiados
- Negociação coletiva
- Pluralidade sindical
- Métodos autocompositivos no Direito do Trabalho
- Recopilação das decisões do Conselho de Liberdade Sindical, da OIT
- Eleições sindicais
- Um algoritmo chamado trabalhador
- Trabalho por aplicativos
- Direito de greve
- Assédio moral, sexual e político
- Direitos humanos
- Relatório do GAET/Ministério da Economia
- Atualização trabalhista: estudo dogmático e crítico
- Sindicalismo e gerações humanas: séculos XX e XXI (*Seminário*)
- **Se preferir, peça para a Excola montar um curso personalizado para sua entidade.**

Coordenador científico:

Gérson Marques (Doutor, professor, Subprocurador-Geral do Trabalho)

Currículo lattes: <http://lattes.cnpq.br/9716751606619741>

LGPD

Orientações para os sindicatos



Rua Monsenhor Bruno, 1153, sl. 1705, Aldeota, Fortaleza-CE | CEP 60.115-191
Fone: (85) 98897-7566 | www.excolasocial.com.br | excolasocial@gmail.com