SECRETARIA DE SEGURANÇA PÚBLICA
UNIVERSIDADE ESTADUAL DE GOIÁS – UEG
COORDENADORIA DE ENSINO
COORDENAÇÃO DE ENSINO PRESENCIAL E DE PÓS-GRADUAÇÃO
CURSO DE ALTOS ESTUDOS EM SEGURANÇA PÚBLICA

ADEMAR RAMALHO DA SILVA FILHO

O ORDENAMENTO JURÍDICO BRASILEIRO E A PROTEÇÃO DOS DADOS PESSOAIS DOS SERVIDORES DO CBMGO

GOIÂNIA-GO

2024

ADEMAR RAMALHO DA SILVA FILHO

O ORDENAMENTO JURÍDICO BRASILEIRO E A PROTEÇÃO DOS DADOS PESSOAIS DOS SERVIDORES DO CBMGO

Artigo apresentado como exigência parcial para conclusão da disciplina Metodologia Científica do Curso de Altos Estudos em Segurança Pública (CAESP) pela Secretaria de Segurança Pública de Goiás e a Universidade do Estado de Goiás, sob a orientação do Prof. Esp. Emerson Divino Gonçalves Ferreira.

GOIÂNIA-GO

2024

O ORDENAMENTO JURÍDICO BRASILEIRO E A PROTEÇÃO DOS DADOS PESSOAIS DOS SERVIDORES DO CBMGO

THE BRAZILIAN LEGAL SYSTEM AND THE PROTECTION OF PERSONAL DATA OF CBMGO SERVERS

Ademar Ramalho da Silva Filho[1]

Emerson Divino Gonçalves Ferreira[2]

Resumo: O foco da pesquisa reside na análise do ordenamento jurídico brasileiro e no processo atual de acesso às fichas funcionais dos servidores do Corpo de Bombeiros Militar (CBMGO). Atualmente, observa-se que perfis de vários servidores do CBMGO estão tendo acesso pleno às informações pessoais de todos os demais servidores do CBMGO, inclusive fichas funcionais e até prontuários médicos. Os prontuários médicos são as anotações mais íntimas e sensíveis, protegidas pelo sigilo médico/paciente assim, indubitavelmente, trazem informações sigilosas sobre o paciente. Já é pacífico o quão prejudicial é o acesso a essas informações, pois elas expõem dependências químicas, alcoolismo, informações privadas de saúde e o acesso indiscriminado a tudo isso pode causar grandes tragédias na vida pessoal do servidor e à toda a Corporação. Esses dados pessoais são protegidos tanto pela Lei Geral de Proteção de Dados, de 2018, como pela própria Constituição Federal, de 1988 e a legislação ordinária que regula a profissão médica. Assim como o prontuário médico, a ficha funcional será estudada nessa pesquisa em seu modelo atual, com todas as informações que contém e será feita uma análise e sugestão, legalmente justificada, de quais autoridades devem ter acesso a essas informações. O sistema de informações é pautado pela melhoria contínua dos processos, através da análise dos procedimentos, recebendo o retorno positivo ou negativo de seus operadores, traçando um caminho de aprendizado técnico que poderá auxiliar em tomadas de decisões da alta gestão institucional.

PALAVRAS-CHAVE: Lei; Constituição Federal; Gestão institucional; Proteção de dados pessoais.

[1] Bacharel em Segurança Pública (2004) com habilitação à Bombeiro Militar. Bacharel em Direito (2005). Especialista em Gestão em Segurança Pública (SSP-GO/UEG). E-mail: ramalhoqoc@gmail.com.

[2] Formado em Educação Física. Especialista em Gestão em Segurança Pública. Especialista em Altos Estudos de Segurança Pública. E-mail: tcbmemerson@gmail.com.

Abstract: The focus of the research lies in the analysis of the Brazilian legal system and the current process of accessing the functional records of Goiás Fire Department CBMGO servers. Currently, it is observed that profiles of several CBMGO servers are having full access to the personal information of all other CBMGO servers, including functional records and even medical records. Medical records are the most intimate and sensitive notes, protected by doctor/patient confidentiality and therefore, undoubtedly, contain confidential information about the patient. It is already clear how harmful access to this information is, as it exposes chemical dependencies, alcoholism, private health information and indiscriminate access to all of this can cause great tragedies in the personal life of the server and the entire Corporation. This personal data is protected both by the General Data Protection Law of 2018 and by the Federal Constitution of 1988 and the ordinary legislation that regulates the medical profession. Just like the medical record, the functional record will be studied in this research in its current model, with all the information it contains and an analysis and suggestion will be made, legally justified, as to which authorities should have access to this information. The information system is guided by the continuous improvement of processes, through the analysis of procedures, receiving positive or negative feedback from its operators, tracing a path of technical learning that can assist in decision-making by senior institutional management.

KEYWORDS: Law; Federal Constitution; Institutional management; Protection of personal data.

SUMÁRIO

INTRODUÇÃO

A privacidade e intimidade do cidadão sempre foi tema caro ao direito, desde tempos remotos. Não deve ser diferente o tratamento conferido às anotações e informações sobre a vida funcional e privada do servidor. Trazendo para a realidade prática da presente pesquisa, observa-se uma falha no controle de acesso às fichas funcionais dos servidores públicos do Corpo de Bombeiros Militar do Estado de Goiás, assim como seu prontuário médico e todas as informações sensíveis guardadas no banco de dados da SSP/GO (Secretaria de Segurança Pública do Estado de Goiás).

No Brasil, a Constituição 1988 e o Código Civil de 2002 (Lei n. 10.406) se referem a privacidade com as expressões *vida privada* e *intimidade.* A Constituição de 1988 contém o termo sigilo, referindo-se ao direito de privacidade das correspondências, das comunicações telegráficas, de dados e das comunicações telefônicas. Corroborando com essa preocupação com a privacidade do cidadão, Ardenghi (2012, p. 238) considera o direito à intimidade como o poder conferido à pessoa de se resguardar de intromissões ao espaço mais reservado de sua existência, assim como "a faculdade de fazer concessões nesse terreno". Só no ano de 2020 entrou em vigor uma lei mais específica para regulamentar a previsão constitucional, a Lei Geral de Proteção de Dados (Lei nº 13.709/18).

O autor deste artigo possui formação jurídica (bacharel em direito), com foco no direito constitucional, objeto de especialização. Atualmente ocupa o cargo de chefe da BM/6 (Seção de Tecnologia da Informação e Comunicações do CBMGO), seção essa que desenvolve os sistemas do CBMGO, além de estabelecer e manutenir toda a rede de computadores da Corporação e a comunicação através dos telefones (telefonia convencional, VoIP e celulares). No exercício dessa função, nos deparamos com um problema preocupante e de urgente solução: os perfis de vários servidores têm acesso pleno às informações pessoais de todos os demais servidores do CBMGO, inclusive fichas funcionais e até prontuários médicos.

Os prontuários médicos indubitavelmente trazem informações sensíveis e sigilosas sobre o paciente. Já é pacífico o quão prejudicial será o acesso a essas informações, pois elas expõem sobre dependências químicas, alcoolismo, informações privadas de saúde e o acesso indiscriminado a essas informações pode causar grandes tragédias na vida pessoal do servidor e em toda a Corporação. Dados esses que são

protegidos tanto pela Lei Geral de Proteção de Dados, de 2018, como pela própria Constituição Federal, de 1988 e a regulamentação a profissão médica.

Assim, como o prontuário médico, a ficha funcional será é abordada nessa pesquisa em seu modelo atual, com todas as informações que contém e em seguida será apresentada uma análise e consequente sugestão de quais autoridades devem ter o acesso a essas informações de todos os servidores do CBMGO.

O tema segurança e tratamento dos dados pessoais está em destaque desde 2020, quando começa a vigorar a LGPD: Um marco na regulamentação sobre dados pessoais no Brasil. A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei n. 13.709, de 14 de agosto de 2018 entrou em vigor em setembro de 2020. Já as sanções previstas na lei tiveram um período maior para adaptação e passaram a valer em agosto de 2021, mas só foram regulamentadas no último mês de fevereiro. Entre as penalidades previstas estão a advertência, a multa de até 2% do faturamento da empresa — limitada a R$ 50 milhões — e o bloqueio dos dados.

Tão preocupante como os aspectos legais, são os aspectos sociais e de relação de trabalho com esse acesso indiscriminado às fichas funcionais dos servidores. A exposição excessiva dos dados abre espaço para problemas diversos com resultados drásticos: um servidor pode ser exposto por ter muitas licenças e dispensas médicas, muitas pensões alimentícias, ou outra causa que lhe confira constrangimento com seus colegas, levando a situações complexas como depressão, assédio moral e demais exposições indevidas.

Como já foi exposto, o acesso e tratamento dos dados pessoais está cada vez mais fácil, tecnológico e dinâmico e os bancos de dados estão cada vez mais seguros, dotados de criptografia de ponta e de difícil acesso clandestino. Esta pesquisa não se justifica pela fragilidade na segurança dos dados e sim na legalidade para o controle de acesso a essas informações pessoais.

Muitos servidores do CBMGO solicitam acesso às fichas funcionais e prontuários médicos por ocuparem funções administrativas na Corporação. Em alguns casos, a concessão se justifica e tem coerência e legalidade, mas em outros são flagrantes de ilegalidade e não existe atualmente uma norma clara que regularize esse acesso aos dados na forma em que eles se apresentam atualmente (portaria ou norma). Portanto, nota-se que faz necessário urgente regulamentar esse acesso e alinhá-lo com a legalidade e os demais princípios constitucionais.

1. HISTÓRIA E EVOLUÇÃO DA COLETA E ARMAZENAMENTO DOS DADOS DOS SERVIDORES PÚBLICOS MILITARES DE GOIÁS

1.1 **A necessidade de coleta de dados pessoais de componentes das instituições militares.**

No início da carreira do autor desse artigo (Curso de Formação de Oficiais PM 2001) as fichas funcionais eram datilografadas e guardadas num arquivo trancado do Comando de Gestão e Finanças - CGF. Quando era necessário alterar algum dado (cancelamento de punição, por exemplo) o servidor do CGF precisava passar um corretivo líquido ou uma faixa preta no registro da punição.

As carreiras públicas, principalmente as policiais e as militares são diferenciadas, pois, após o ingresso, o servidor público passa a ter poderes de polícia (guarda e proteção das pessoas e dos bens) e de fiscal do estado (vistorias, blitz, dentre outras ações de fiscalização), além do porte de arma inerente ao exercício da função. Como o estado está outorgando inestimável função e grandes responsabilidades, é necessário conhecer bem o cidadão aprovado no concurso público antes de sua investidura no cargo.

Para Hely Lopes Meirelles: “Poder de polícia é a faculdade de que dispõe a Administração Pública para condicionar e restringir o uso e gozo de bens, atividades e direitos individuais, em benefício da coletividade ou do próprio Estado.” (Meirelles, p. 103)

A administração pública não precisa de consentimento para tratar dados pessoais, mas deve informar ao titular dos dados a finalidade e a forma como os dados serão tratados. Para isso, é feita uma investigação de vida pregressa, pelos órgãos de inteligência e são colhidas certidões, informações pessoais, psicossociais, familiares, dentre outras que formam o perfil da pessoa para a análise e ingresso na carreira. A partir dessas informações iniciais começam a se formar os dados que constarão na ficha funcional do bombeiro militar e que o acompanharão durante toda a sua carreira.

1.2 Evolução na coleta, tratamento e acesso aos dados (sistemas atuais de informática) informações pessoais e de restrito acesso contidas na ficha funcional e no prontuário médico.

A tecnologia mudou toda a forma com que registramos, processamos e acessamos os dados. Essa mudança foi uma revolução extremamente positiva, trazendo dinamicidade e até mais segurança no tratamento dos dados no mundo da tecnologia da informação em que vivemos.

Em outros tempos, um simples incêndio apagaria ou danificaria permanentemente esses dados. Porém, esse poder, segurança e rapidez no tratamento dos dados carrega também grande responsabilidade no que tange à liberação seletiva, legal e responsável ao acesso aos dados. Se o concorrente à mesma graduação ou posto tem acesso a essas informações, poderá fazer muito para prejudicar a boa e honesta disputa. Dispensas médicas, punições, pontos fracos, tudo isso está exposto na ficha do servidor e, quando trabalhado com intenção nociva, pode até revelar as senhas e demais informações personalíssimas do servidor, pois lá contém nome dos filhos, pais, esposa, marido, datas de nascimento, endereço, cursos, elogios, punições e muitas outras informações. O acesso indiscriminado a essas informações representa um perigo especial para nós, servidores da segurança pública, que muitas vezes enfrentamos o crime e nos deparamos constantemente com confrontos diretos, sujeitos à retaliação por parte dos criminosos e do crime organizado.

Nesse sentido, nos capítulos a seguir será exposta toda a legislação e doutrina brasileira existente na atualidade para garantir uma forma legal de proteger os dados do servidor público do CBMGO, visando manter a disputa saudável na ascensão à carreira militar e, principalmente proteger e respeitar a intimidade e privacidade dos bombeiros militares de Goiás, buscando soluções práticas para esse problema jurídico e, antes de tudo, social.

2. A CONSTITUIÇÃO FEDERAL BRASILEIRA E O DIREITO INTERNACIONAL COMO FORMA DE PROTEÇÃO DA PRIVACIDADE DO CIDADÃO

2.1 A Constituição Federal Brasileira e os sistemas de informações do Estado de Goiás quanto à coleta, o acesso e o uso dos dados dos servidores.

Alguns direitos fundamentais estão garantidos na própria Constituição Federal Brasileira de 1988 (CF/88), dentre eles estão direitos humanos básicos, como o direito à

privacidade, inclusive digital, inserido no diploma legal através da Emenda Constitucional 115/2022, que elenca a proteção de dados pessoais como garantia fundamental e evolução do direito com as novas tecnologias: “(...) os Direitos protetivos dos seres humanos, os quais evoluíram no tempo, a fim de se encontrar o melhor conceito que abarcasse todos os Direitos inerentes à pessoa humana” (Oliveira, 2013, p. 19).

Com tamanha importância para o ser humano, o direito à privacidade está explicitamente enunciado no artigo 12 da Declaração Universal dos Direitos Humanos (Universal Declaration of Human Rights): “Ninguém será sujeito a interferências na sua vida privada, família, lar ou na sua correspondência, nem a ataque à sua honra e reputação.”

Por conseguinte, esses direitos foram fortalecidos pelo Positivismo, passando a integrar, de forma expressa, o Ordenamento Jurídico, por meio das Constituições e Normas Infraconstitucionais da época; recebendo, assim, a designação de Direitos Humanos e Direitos Fundamentais; o que, mais tarde, devido à sua grande importância e necessidade universal, também, passaram a integrar o conteúdo de Convenções e Tratados Internacionais (Oliveira, 2013, p. 19).

Contudo, devido às grandes divergências conceituais e culturais, principalmente as religiosas, que imperavam o dado momento histórico, foi necessário que se buscasse, com aprofundamento, uma teoria comum a todos, para um melhor conceito de pessoa e de sua dignidade. Discussão filosófica que originou algumas teorias que merecem apreço (Comparato, 2010, p. 31), tais como:

> • Teoria de Cunho Religioso – buscava a melhor interpretação a respeito da identidade de Cristo, se a da ortodoxia ou da heterodoxia (Comparato, 2010, p. 31); • Teoria da Composição Biológica – considerava que o ser humano era composto de corpo e espiritualidade; distinguindo, assim, uns dos outros, mas também os tornavam semelhantes entre si; gerando uma interpretação pautada no princípio da igualdade (Comparato, 2010, p. 32); • A Teoria Kantiana - instituía que apenas o ser humano era um ser racional, ou seja, dotado de razão, e, representava um princípio objetivo, onde previa que as pessoas deveriam viver em condições de autonomia, tendo sua dignidade como um fim em si mesmo; porém, respeitando à individualidade de cada um diante das Leis (Comparato, 2010, p. 33 - 35); • A Teoria do Século XX - identificou que o ser humano não é apenas aquilo que se reflete em sua conduta, diante do convívio em sociedade; mas sim, um ser constituído de uma essência pessoal e individual de cada um; vindo a reconhecer a singularidade de cada indivíduo que é portador de um valor próprio, ao passo que sua existência é inconfundível e insubstituível a qualquer outro ser (Comparato, 2010, p. 39).

Foi logo após a grande afirmativa de Kant que houve a transformação dos fundamentos da Ética, pautados no princípio da dignidade da pessoa humana; vindo a ocorrer, então, a última teoria histórica, acima mencionada, que reconheceu a verdadeira capacidade do homem e sua unicidade quanto ao seu modo de ser e agir; onde se concentra todo o universo axiológico. Além disso, que, contrária às Normas do Direito natural, passam a reconhecer que o homem é capaz de direcionar-se, de acordo com as Normas de Direito, de forma valorativa e em consonância com a Ética moral (Comparato, 2010, p. 37 - 38).

Desse modo, é possível afirmar que o Período Axiológico teve um papel importantíssimo na essência histórica sobre a elaboração do conceito de pessoa e dos Direitos do homem; bem como, na origem dos Direitos Humanos, quando foi possível extrair os primeiros indícios do princípio inerente a cada indivíduo; também, norteador desses direitos, qual seja a dignidade da pessoa humana (Comparato, 2010, p. 43).

Nesse sentido, de acordo com Monteiro (2018) A Lei de Proteção de Dados (LGPD) estabelece a gestão do consentimento para evitar uso indevido; logo, um dado pessoal publicado por força da Lei de Acesso à Informação (LAI), que também será abordada e discutida no âmbito do serviço público, do princípio da publicidade versus direito de privacidade do servidor público. Esses dados então só podem ser tratados para finalidade específica da transparência, não podem ser disponibilizados para consulta, a não ser em casos específicos de necessidade funcional justificada na lei. O fato de estar disponível para certas autoridades, não transforma um dado pessoal em dado público.

Assim, o conjunto de dados pessoais abarca qualquer informação identificada ou identificável, ou seja, qualquer informação que possibilite identificar ou tornar identificável uma pessoa física será um dado pessoal. Esses dados vão além do número de CPF, RG, não se trata apenas de dados concretos, contemplam, também, os dados de caráter subjetivo como dados financeiros, dados de hábitos de consumo, características físicas, registros de históricos de saúde, identificadores eletrônicos, entre outros.

A Carta Magna brasileira trata dos direitos fundamentais do cidadão, dentre eles o direito à privacidade (inclusive de dados e informações) e ao acesso às informações de interesse pessoal, coletivo ou geral. Nesse sentido, o servidor público cujos dados contam nos sistemas de informações do estado, tem direito não só ao sigilo dos seus dados pessoais, como também o acesso aos dados de seu interesse particular, a não ser

que estejam de alguma forma sob sigilo momentâneo (para não interferir em uma sindicância investigativa, por exemplo).

> 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:
>
> (...)
>
> XXXIII - todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado; (Regulamento) (Vide Lei nº 12.527, de 2011)

O Supremo Tribunal Federal é a corte que decide, em última instância, sobre as questões de constitucionalidade. Quanto ao sigilo dos dados do servidor público, no mais recente entendimento do STF (Supremo Tribunal Federal), o compartilhamento dos dados do servidor público deve ser limitado ao mínimo necessário, para atender a finalidade informada, com controle rigoroso de acesso. Também deve cumprir integralmente os requisitos, as garantias e os procedimentos estabelecidos na Lei Geral de Proteção de Dados (LGPD – Lei 13.709/2018) compatíveis com o setor público. Entre eles, citou mecanismos rigorosos de controle de acesso ao Cadastro Base do Cidadão, publicidade do compartilhamento ou do acesso a banco de dados pessoais e fornecimento de informações claras e atualizadas sobre previsão legal, finalidade e práticas utilizadas.

3. O ACESSO AOS DADOS PESSOAIS DOS SERVIDORES DO CBMGO

3.1. Os mecanismos de proteção e sigilo de dados na legislação, doutrina e jurisprudência brasileira, com foco na Lei Geral de Proteção de Dados (LGPD), de 2018.

A Lei Geral de Proteção de Dados (Lei nº 13.709/18) entrou em vigor no ano de 2020 e desde então tem causado grandes debates e discussões técnicas nos mais diversos ambientes profissionais, principalmente no que tange à área do Direito, da Tecnologia da Informação e Administração Pública, foco desse artigo científico. Entrando em vigor no dia 18 de setembro de 2020, trata-se de um dispositivo legal

novo, considerando o universo jurídico, portanto ainda não há conhecimento sedimentado. Porém já vem sendo discutido por grandes doutrinadores da atualidade, assim como tem sido objeto de inúmeras decisões judiciais, formando assim uma jurisprudência consolidada nesses últimos quatro anos.

A LGPD não foi pensada para as peculiaridades das relações de trabalho, é uma lei de caráter genérico e amplo, mais voltada para questões consumeristas, como expresso em seu art. 2º atua para defender a privacidade, a autodeterminação informativa, a liberdade de expressão, de informação e de opinião (Giuntini, 2021, p. 8).

A LGPD trata de algumas hipóteses para o manuseio ou divulgação dos dados em seus artigos **7º** e 11:

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
>
> I - mediante o fornecimento de consentimento pelo titular;
>
> II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
>
> III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
>
> (...)
>
> VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
>
> III - para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;
>
> VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
>
> (...)
>
> Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
>
> I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
>
> II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
>
> a) cumprimento de obrigação legal ou regulatória pelo controlador;
>
> b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
>
> (...)
>
> e) proteção da vida ou da incolumidade física do titular ou de terceiro;
>
> f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou
>
> (...)

Percebe-se que, segundo o inciso I do artigo 7º da LGPD, é necessário o consentimento ou o fornecimento dos dados pelo seu titular e a própria citada lei trás

exceções taxativas para o acesso aos dados pessoais. Além disso, a LGPD prevê a situação do tratamento de dados pessoais pelas pessoas jurídicas de direito público, que deverá ser realizado para o atendimento de sua finalidade pública e na busca do interesse público (art. 23 da LGPD):

> Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:
>
> I – sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos;
> (...)
> III – seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei.
> III – seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei; e (Redação dada pela Lei nº 13.853, de 2019) Vigência
> (...)

A Lei de Acesso à Informação – LAI (Lei 12.527/2011) tem o objetivo de garantir o acesso a informações, regulamentando então o acesso às informações, direito este já garantido pela Constituição Federal de 1988. Porém o direito a que se refere essa lei é o de receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral:

> Art. 31. O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais.
>
> § 1º As informações pessoais, a que se refere este artigo, relativas à intimidade, vida privada, honra e imagem:
>
> I - terão seu acesso restrito, independentemente de classificação de sigilo e pelo prazo máximo de 100 (cem) anos a contar da sua data de produção, a agentes públicos legalmente autorizados e à pessoa a que elas se referirem; e
>
> II - poderão ter autorizada sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem.
>
> § 2º Aquele que obtiver acesso às informações de que trata este artigo será responsabilizado por seu uso indevido.
>
> § 3º O consentimento referido no inciso II do § 1º não será exigido quando as informações forem necessárias:
>
> I - à prevenção e diagnóstico médico, quando a pessoa estiver física ou legalmente incapaz, e para utilização única e exclusivamente para o tratamento médico;
>
> II - à realização de estatísticas e pesquisas científicas de evidente interesse público ou geral, previstos em lei, sendo vedada a identificação da pessoa a que as informações se referirem;

> III - ao cumprimento de ordem judicial;
>
> IV - à defesa de direitos humanos; ou
>
> V - à proteção do interesse público e geral preponderante.
>
> § 4º A restrição de acesso à informação relativa à vida privada, honra e imagem de pessoa não poderá ser invocada com o intuito de prejudicar processo de apuração de irregularidades em que o titular das informações estiver envolvido, bem como em ações voltadas para a recuperação de fatos históricos de maior relevância.

Os agentes públicos legalmente autorizados, aos quais se refere o inciso I do artigo 31 da LAI são os que guardam nexo de causalidade entre a permissão do acesso e o estrito cumprimento do dever funcional. Este cuidado se dá pela natureza privada dos dados aqui tratados, pois a ficha funcional e o prontuário médico contêm informações pessoais e íntimas. Em alguns casos essas informações foram publicadas em Boletim Geral ou Boletim Reservado, mas além das informações serem exclusivamente sobre a pessoa pesquisada no sistema, elas constituem uma coletânea com todas as informações públicas ou não sobre determinado servidor.

3.2 A segurança digital dos sistemas da SSPGO (possibilidade de invasão clandestina e coleta de dados).

Os dados armazenados pela SSPGO (Secretaria de Segurança Pública de Goiás) no SICAD (Sistema de Cadastro) e no SISSAUDE (Sistema de Saúde) são assegurados pelo banco de dados Oracle, que é referência mundial em segurança de dados e controla de acesso criptografados.

O banco de dados Oracle: “Assegura proteção contra ataques externos e usuários internos mal-intencionados. Aplica automaticamente atualizações de segurança durante a própria operação para se proteger contra ataques cibernéticos e automaticamente criptografa todos os dados.” <disponível em: https://revistasegurancaeletronica.com.br/oracle-lanca-primeira-solucao-autonoma-do-mundo-de-banco-de-dados-na-nuvem/, acesso em 04/10/2024, 15:46 h>

A segurança dos dados da SSP deve ser absoluta, recentemente a seção de TI e Comunicações do Corpo de Bombeiros providenciou a retirada dos Boletins Gerais do site da Corporação, pois o sistema de dados utilizado pelo WordPress é bastante vulnerável, ao contrário do banco de dados Oracle, que contém originariamente os boletins do CBMGO e é consideravelmente mais seguro e confiável.

“WordPress é um sistema livre e aberto de gestão de conteúdo para internet, baseado em PHP com banco de dados MySQL e MariaDB, executado em um servidor interpretador, voltado principalmente para a criação de páginas eletrônicas e blogs online.” <disponível em: https://wordpress.com/pt-br/, acesso em 04/10/2024, 15:38 h>

Essa medida prova o quão relevante e sensível são os assuntos tratados em nossos boletins, principalmente no que tange ao controle de acesso e divulgação, pois somos parte integrante e pungente do Sistema de Segurança Pública do Estado de Goiás, com atribuições, responsabilidades, missões e poder de polícia.

3.3 **Autoridades que necessitam ter acesso “PLENO” às fichas dos servidores do CBMGO e por quais dispositivos legais tal acesso se justifica.**

Como foi visto e justificado no item 3.1 deste estudo, de acordo com a LGPD, o tratamento de dados pessoais pelo Poder Público pode ser feito para cumprir obrigações legais ou regulatórias. No entanto, algumas regras devem ser seguidas, como:

- O compartilhamento de dados deve ser limitado ao mínimo necessário;
- Deve ser cumprida a LGPD e os procedimentos compatíveis com o setor público;
- Deve haver mecanismos de controle de acesso;
- Deve haver publicidade do compartilhamento ou do acesso aos dados;
- Deve haver informações claras e atualizadas sobre a previsão legal, finalidade e práticas utilizadas.

Nesse sentido, algumas autoridades exercem funções dentro do Corpo de Bombeiros Militar que exigem acesso irrestrito às fichas funcionais de todos os servidores da Corporação, isso não engloba o acesso aos prontuários médicos, que serão tratados no item 3.5 desse artigo.

O comando da Corporação (Comandante Geral, Subcomandante Geral e Chefe do Estado Maior Geral) está diretamente relacionado funcionalmente com a gestão de toda a tropa do CBMGO, devendo ter acesso irrestrito a ficha de todos os servidores sob seu comando para o acionamento, comandamento e assessoramento de todos os militares sob seu comando.

A Assessoria do Comando da Corporação é composta por militares bacharéis em direito que prestam assessoria ao Comando Geral. Sendo assim a função de todos os

seus integrantes necessita de acesso total às informações de todos os militares, contidas nas fichas funcionais, para prevenir ou resolver eventuais problemas jurídicos que envolvam a Instituição ou seus componentes. Muitas vezes é necessário, para o exercício da função, constar extratos de informações relevantes da ficha funcional nos processos jurídicos ou administrativos.

Nesse mesmo sentido, todos os militares do Comando de Correição e Disciplina necessitam do acesso a todas as fichas funcionais dos militares da Corporação, pois o CCD é responsável pela manutenção da disciplina em todo o CBMGO e abertura dos processos administrativos. Por lidar com assuntos sensíveis (punição, exclusão, dentre outros) os militares do CCD, assim como os da Assessoria Jurídica e os da BM2 (inteligência) já são previamente selecionados com cautela e baseado nos conhecimentos, principalmente jurídicos inerentes às funções exercidas.

Os militares da BM/2 (Seção de Inteligência) são responsáveis pelo assessoramento nas tomadas de decisão do Comando e para isso exercem a essencial função de investigação e coleta de informações, assim como elaboração de relatórios de inteligência. A função de inteligência requer extrema disciplina e comprometimento no tratamento dos dados e, como assessores diretos do Comando, necessitam do acesso irrestrito às fichas funcionais de todos os servidores da Corporação, inclusive seus superiores, que podem ser alvo de investigação sob orientação do próprio Comando da Instituição.

A Academia Bombeiro Militar é responsável pela formação, aperfeiçoamento e controle dos especialistas, assim como diagnóstico de necessidade de cursos de formação, especialização, assim como inclusão de efetivo. No exercício dessa função, o Comandante da Academia Bombeiro Militar assessora diretamente o Comando Geral e nessa função necessita do acesso pleno às fichas de todo o efetivo do CBMGO, assim como o subcomandante da ABM e o oficial responsável pelo RH (SAAD).

Nesse mesmo sentido, o Comandante de Gestão e Finanças, o subcomandante e o oficial responsável pela folha de pagamento, o oficial responsável pelo DCP (Departamento de Controle de Pessoal) e o oficial responsável pelo Boletim Geral, que têm inegável vínculo funcional com o acesso a todas as fichas pessoais dos servidores do CBMGO. No CGF são feitas as publicações, assinadas as portarias de transferência e exercida toda a função de folha de pagamento da Corporação.

Todas as autoridades supracitadas têm a possibilidade de indicar assessores que também detenham o acesso irrestrito às fichas funcionais de todos os servidores da Corporação, desde que o acesso desses servidores seja justificado pela função de assessoramento e seja temporário, restrito ao período em que esse servidor exerça efetivamente essa função.

Durante a vigência na função, os oficiais da CPP (Comissão de Promoção de Praças) e da CPO (Comissão de Promoção de Oficiais) deverão ter acesso à todas as fichas funcionais da Corporação, com o único intuito de contagem de pontuação e tempo de serviço dos candidatos à promoção.

3.4 Autoridades que necessitam ter acesso "RESTRITO" às fichas dos servidores do CBMGO sob seu comando e por quais dispositivos legais tal acesso se justifica.

Assim como algumas autoridades devem ter acesso irrestrito a todas as fichas dos servidores da Corporação, outras autoridades necessitam do acesso irrestrito às fichas dos servidores sob seu comando e essas informações são exclusivamente para o exercício de suas funções.

O comandante de uma Unidade Militar, seja administrativa ou operacional e os Comandantes Regionais precisam acessar informações pessoais e profissionais dos seus comandados. Isso possibilita uma gestão dinâmica dos recursos humanos, aproveitando os especialistas e os formados em determinadas áreas (direito, TI, engenharia, dentre outras) e todas essas informações estão contidas de forma objetiva na ficha funcional de seus militares.

Além disso, o comandante é responsável pelo bem estar da tropa e pelo alcance de seus militares, devendo ter fácil acesso a todos os dados para gerir e cuidar dos comandados, inclusive em casos de emergências públicas ou pessoais dos servidores sob seu comando.

O oficial ou praça graduado responsável pela seção de RH (SAAD) também deve ter o acesso garantido às informações de todos os militares da Unidade, pois ele é o responsável pelas publicações em ficha, em boletim, guarda e tratamento desses dados com fidedignidade.

Ambas as funções aqui elencadas trazem um inegável vínculo funcional com a necessidade de acesso aos dados dos servidores, isso legitima o atributo público e funcional do acesso que lhe é garantido.

3.5 Prontuários médicos dos militares, regulamentação específica e acessos autorizados.

Os prontuários médicos, contidos no SISSAUDE são os dados mais sensíveis sobre o servidor. Existe uma legislação própria que garante que esses dados são de acesso exclusivo dos médicos.

Não existem exceções para o tratamento desses dados, pois neles contém informações sobre dependências químicas, confidências pessoais médico/paciente, dentre outras informações que trariam uma exposição irreparável à imagem do servidor, trazendo consequências desastrosas no caso de divulgação desses dados.

O Código Penal Brasileiro (Decreto-Lei 2.848, DE 7 DE DEZEMBRO DE 1940) traz como crime as seguintes situações:

> Art. 153 - Divulgar alguém, sem justa causa, conteúdo de documento particular ou de correspondência confidencial, de que é destinatário ou detentor, e cuja divulgação possa produzir dano a outrem:
>
> Pena - detenção, de um a seis meses, ou multa, de trezentos mil réis a dois contos de réis.
>
> § 1º Somente se procede mediante representação.
>
> § 1o-A. Divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública:
>
> Pena – detenção, de 1 (um) a 4 (quatro) anos, e multa.
>
> § 2o Quando resultar prejuízo para a Administração Pública, a ação penal será incondicionada.
>
> Violação do segredo profissional
>
> Art. 154 - Revelar alguém, sem justa causa, segredo, de que tem ciência em razão de função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a outrem:
>
> Pena - detenção, de três meses a um ano, ou multa de um conto a dez contos de réis.
>
> Parágrafo único - Somente se procede mediante representação.

Portanto, violar, acessar ilegalmente ou divulgar dado pessoal e sigiloso, como o prontuário médico) é crime, constante no Título I (Dos Crimes Contra a Pessoa), Capítulo VI (Dos Crimes Contra a Liberdade Individual) do Código Penal Brasileiro e a

punição é mais severa se a divulgação é de informações sigilosas ou reservadas, contidas ou não nos sistemas ou banco de dados da Administração Pública.

O prontuário médico pode ser acessado exclusivamente pelo médico ou próprio paciente ou representante legal especificamente constituído para esse propósito, pois constitui direito fundamental à intimidade, previsto na Constituição Federal brasileira (art. 5º, X, CF/88), por esse motivo as informações nele contidas são sigilosas. No entanto, como todo direito, o direito à intimidade também não é absoluto, comportando três restrições trazidas pelo artigo 89 do Código de Ética Médica (Resolução CFM n° 2.217, de 27 de setembro de 2018, modificada pelas Resoluções CFM nº 2.222/2018 e 2.226/2019):

> Art. 89. Liberar cópias do prontuário sob sua guarda exceto para atender a ordem judicial ou para sua própria defesa, assim como quando autorizado por escrito pelo paciente.
>
> § 1º Quando requisitado judicialmente, o prontuário será encaminhado ao juízo requisitante.
>
> § 2º Quando o prontuário for apresentado em sua própria defesa, o médico deverá solicitar que seja observado o sigilo profissional.

I – Atender à ordem judicial:

A primeira hipótese de afastamento do sigilo sobre o prontuário é no caso de ordem judicial. De fato, atualmente são muitos os processos judiciais em que magistrados determinam ao médico o envio de prontuários aos autos do processo.

Importante salientar que, a respeito dessa primeira hipótese, a ordem deve emanar de um juiz de direito em meio a um processo judicial. Isso significa que o médico detentor do prontuário não deve, nem pode, atender ordem emanada de outras autoridades julgadoras em processos não judiciais. Por exemplo, caso esteja em trâmite um processo ético-disciplinar contra um médico, as autoridades julgadoras do CFM (Conselho Federal de Medicina) e do CRM (Conselho Regional de Medicina) não têm poder para determinar a apresentação de prontuários médicos. Outro exemplo é um juiz arbitral em um processo de mediação e arbitragem (não judicial), que também não possui autoridade para determinar a apresentação de prontuários.

Uma última observação quanto ao fornecimento de prontuário para atendimento de determinação judicial é que o prontuário deve ser encaminhado pelo médico diretamente ao juízo requisitante, não podendo ser entregue a intermediários.

II - Defesa do médico

A segunda hipótese de afastamento do sigilo do **prontuário médico** ocorre quando um médico necessita se defender. Embora a lei não forneça muitos detalhes, entende-se que essa hipótese trata da defesa do médico contra acusações que ele esteja sofrendo em processos administrativos ou judiciais. Portanto, a apresentação do prontuário pelo médico pode ocorrer tanto em um processo judicial quanto em um processo ético-profissional em trâmite no CRM ou no CFM, por exemplo.

Um detalhe importante nessa segunda hipótese é a necessidade de o médico requerer à autoridade julgadora, antes de apresentar o atestado, que seja observado no processo o sigilo processual.

III - Autorização do paciente

Por fim, a terceira hipótese de restrição do sigilo do **prontuário médico** diz respeito à possibilidade de o próprio paciente autorizar por escrito a liberação de cópias. Nesse ponto, é necessário observar o princípio da razoabilidade e da proporcionalidade, no sentido de que as autorizações para compartilhamento de prontuários devem ser específicas e pontuais, e não genéricas para qualquer situação, sob pena de o médico atentar contra o dever de sigilo profissional.

4. SUGESTÕES DE SOLUÇÕES PRÁTICAS A SEREM APLICADAS NO ÂMBITO DO CBMGO QUANTO AO ACESSO AOS DADOS PESSOAIS DOS SERVIDORES

4.1 Acesso ao Boletim Geral Reservado.

O BGR (Boletim Geral Reservado) contém informações sensíveis, que não deveriam ser disponibilizadas a qualquer militar que descobrisse a senha de acesso (que já é conhecida por quase todo o efetivo do CBMGO). Contendo punições, motivos detalhados e outros assuntos sensíveis, o BGR só deveria estar disponível aos militares que exercem função de Comando, Subcomando ou Chefia. Isso não contraria a LAI (Lei de Acesso à Informação), pois qualquer militar que esteja citado no BGR pode solicitar o acesso a este documento formalmente, expondo esses justificáveis motivos. Para

algum assunto relacionado ao servidor ser publicado no BGR, o mesmo sempre terá ciência, inclusive do número do BGR, consultando sua ficha funcional.

4.2 Proposta de alteração no SICAD.

O sistema atual que contém as fichas funcionais é o SICAD e esse sistema trás quatro níveis possíveis de acesso às fichas funcionais da Corporação:

I- Acesso apena à ficha funcional do próprio servidor;
II- Acesso às fichas funcionais de todos os servidores de uma Unidade Militar;
III- Acesso às fichas funcionais de todos os servidores de um Comando Regional;
IV- Acesso a todas as fichas funcionais de Corporação.

Nesse contexto, propõe-se a seguinte alteração no SICAD: Exceto para os servidores que têm nível de acesso I (apenas a própria ficha funcional), os demais servidores que acessem as fichas funcionais de terceiros deveriam receber o arquivo em formato .PDF contendo marca d´água com o número do CPF de quem acessou, assim se o documento for utilizado indevidamente, sua origem será de fácil identificação.

Atualmente o sistema MPORTAL da SSPGO já possui esse dispositivo de segurança, pois o mesmo também contém dados sensíveis dos cidadãos e seu uso indevido seria ilegal da mesma forma.

Os prontuários médicos, por sua vez, que devem ser acessados apenas pelos médicos e estão contidos no SISSAUDE, devem ter o mesmo nível de segurança, contendo todos a marca d´água com o CPF do profissional médico que o acessou. Isso garante uma cautela extra com os dados mais sensíveis dos servidores / pacientes.

CONSIDERAÇÕES FINAIS

Diante de toda a pesquisa bibliográfica realizada, foram expostos os mecanismos de proteção e sigilo de dados na legislação, doutrina e jurisprudência brasileira, com

foco na Lei Geral de Proteção de Dados (LGPD), de 2018. Com atuação jurídica recente, a LGPD ainda não está totalmente contemplada nos mecanismos de prevenção ao acesso indevido de informações sensíveis, tanto no setor público como no privado. Isso gera além do desconforto para o servidor exposto, pode causar uma série de processos administrativos e judiciais, buscando reparação ou indenização pela exposição indevida.

O intuito dessa pesquisa é evitar problemas institucionais futuros, sugerindo a regulamentação do acesso já existente aos sistemas que contém informações sensíveis na Corporação (SICAD e SISSAUDE), pois eles contém dados personalíssimos como endereço, número de documentos, familiares, punições, dependências químicas, intimidades e toda uma gama de informações que só dizem respeito à pessoa ou a servidor que exerça uma função específica que respalde e fundamente o acesso, como as autoridades elencadas no terceiro capítulo deste artigo.

Portanto, diante do deste cenário, sugere-se ao comando do CBMGO a publicação de duas portarias, uma regulamentando e restringindo o acesso às fichas funcionais dos bombeiros no SICAD e outra regulamentando e restringindo o acesso aos prontuários médicos, que devem ser acessados exclusivamente pelos médicos e pelo próprio paciente envolvido, de acordo com as autoridades e níveis de acesso elencados no capítulo 3.

Nesse sentido, e à luz da LGPD, sugere-se também que conste marca d´água contendo o CPF de quem acessou nos arquivos PDF gerados pelo SICAD e nos gerados pelo SISSAUDE, tecnologia já utilizada com sucesso pelo sistema MPORTAL/SSPGO, a qual dificultaria o vazamento indevido dos dados contidos nas fichas funcionais e prontuários médicos, pois o servidor que eventualmente vazar a informação terá sua identificação no documento gerado.

Estamos na era da informação, com ferramentas seguras e dinâmicas, bancos de dados avançados, criptografia de ponta e legislação robusta para a proteção dos dados pessoais. Portanto, cabe-nos aplicar a legislação nos sistemas existentes no CBMGO. Assim, as sugestões contidas no quarto parágrafo deste artigo, se acatadas, aumentariam consideravelmente a segurança dos dados pessoais dos servidores, sem o emprego de recursos ou tecnologias extras, apenas com a devida regulamentação automatizada dos acessos, pois apenas servidores com funções devidamente publicadas e regulamentadas por portaria teriam o acesso aos dados pessoais dos servidores do CBMGO.

REFERÊNCIAS

ARDENGHI, Régis Schneider. **Direito à vida privada e direito à informação: colisão de direitos fundamentais**. Revista da ESMESC, v. 19, n. 25, p. 227-251, 2012.

ÁVILA. Humberto. **Teoria dos Princípios – da definição à aplicação dos princípios jurídicos.** 9ª ed. São Paulo: Malheiros, 2009.

BRASIL. **Constituição da República Federativa do Brasil**. Brasília: Senado, 1988. 168p.

BRASIL. Lei n. 10.406, 2002. **Código Civil Brasileiro.**

BRASIL. Lei n. 13.709, 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD).**

CARVALHO FILHO, José dos Santos. **Manual de Direito Administrativo.** 23ª ed. Rio de Janeiro: Lumen Juris, 2010.

CASADO FILHO, Napoleão. **Direitos Humanos e Fundamentais.** Coleção Saberes do Direito, vl. 57, São Paulo: Editora Saraiva, 2012.

CERVO, Amado Luiz; BERVIAN, Pedro Alcino. **Metodologia científica.** 4 ed. São Paulo : Makron Books, 1996. 209 p.

CONSELHO FEDERAL DE MEDICINA. **Código de Ética Médica.** Resolução CFM n° 2.217, de 27 de setembro de 2018, modificada pelas Resoluções CFM nº 2.222/2018 e 2.226/2019

COTRIN, Gilberto. **Direito Fundamental: Instituições de direito público e privado**. São Paulo: Saraiva, 2009.

FACHIN, O. **Fundamentos de metodologia.** 3. ed. São Paulo: Atlas, 2001.

GIUNTINI, Adriana...[et al.]. **LGPD nas relações de trabalho [livro eletrônico]**. – 1.ed. – Salvador, BA : Motres, 2021.

HENRIQUES, Antônio e MEDEIROS, João Bosco. **Monografia no Curso de Direito: Trabalho de Conclusão de Curso.** São Paulo: Atlas, 1999.

LEITE, Carlos Henrique Bezerra. **Direitos Humanos**. 2. ed. Rio de Janeiro: Editora Lumen Juris, 2011.

MARCONI, Mariana de Andrade; LAKATOS, Eva Maria. **Metodologia Científica.** São Paulo: Atlas, 1986.

MARCONI, Mariana de Andrade; LAKATOS, Eva Maria. **Técnicas de pesquisa.** 3ed. São Paulo : Atlas, 1996. 231 p.

MAZZA, Alexandre. **Manual de direito administrativo.** 3. ed. São Paulo: Saraiva, 2013.

MEIRELLES, Hely Lopes. **Direito Administrativo Brasileiro.** 37ª ed. Malheiros, 2011.

MONTEIRO, Renato Leite. **Existe um direito à explicação na Lei de Proteção de Dados do Brasil?** Instituto Igarapé – Artigo Estratégico, Rio de Janeiro, n. 39, dez. 2018.

OLIVEIRA, Erival da Silva. **Direito Constitucional / Direitos Humanos.** 4. ed., rev. e atual. São Paulo: Editora Revista dos Tribunais, 2013.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Declaração Universal dos Direitos Humanos**, 1948. Disponível em: <https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos>. Acesso em: 10 out. 2024.

PIOVESAN, Flávia. **Direitos Humanos e o Direito Constitucional Internacional**. 14. ed., rev. e atual. São Paulo: Editora Saraiva, 2013.

SANTOS, João Almeida; PARRA FILHO, Domingos. **Metodologia científica.** São Paulo: Futura, 1998. 277 p.