

Artigo 154-A do Código Penal: entenda o crime de invasão de dispositivo informático e suas penas

escrito por Dr. Ademilson Carvalho Santos | 25/10/2026



O artigo 154-A do Código Penal tipifica o crime de invasão de dispositivo informático alheio mediante violação de mecanismo de segurança, com pena de reclusão de 3 meses a 1 ano e multa, agravada em até metade se houver obtenção, alteração ou destruição de dados.

Enfrentar uma investigação policial ou ver um familiar sob acusação criminal traz incertezas profundas sobre os riscos de prisão, a dosimetria das penas e as garantias do devido processo legal. O **artigo 154-A do Código Penal** aborda o crime de invasão de dispositivo informático, cuja conduta envolve o acesso indevido a sistemas alheios com o fim ilícito.

Conhecer os elementos do tipo penal, as penas previstas e as causas de aumento é fundamental para a adequada defesa técnica e para garantir a observância dos direitos constitucionais do investigado ou acusado neste contexto delicado.

Conte com a Ademilson Carvalho Advocacia Especializada para esclarecer dúvidas, identificar nulidades e construir estratégias de defesa criminal eficientes em casos relacionados ao artigo 154-A do Código Penal.

Conceito do crime, bem jurídico tutelado e previsão legal no Código Penal

O **artigo 154-A do Código Penal (Decreto-Lei nº 2.848/1940)** tipifica a invasão de dispositivo informático, conduta que consiste no acesso não autorizado a sistemas eletrônicos ou dispositivos tecnológicos alheios, caracterizando uma intrusão indevida no ambiente digital de terceiros. Trata-se de um crime material que protege diretamente o bem jurídico da **segurança da informação e a intimidade informática**, resguardando o patrimônio imaterial do titular do dispositivo contra ilícitas intervenções.

O bem jurídico tutelado abrange a inviolabilidade dos sistemas computacionais, a confiabilidade, a integridade dos dados e o sigilo das informações armazenadas, elementos essenciais na sociedade digital contemporânea e para a ordem econômica e social.

Previsão Legal e Natureza Jurídica

Este tipo penal foi introduzido pela Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, adaptando o Código Penal para a repressão das novas formas de criminalidade cibernética. A norma estabelece, no caput do **artigo 154-A**, que é crime invadir dispositivo informático alheio, mediante violação indevida de mecanismo de segurança, para obter, adulterar ou destruir dados ou informações sem autorização.

Além do caput, a legislação prevê no § 1º a majorante na hipótese de obtenção, adulteração ou destruição de dados ou informações, e no § 2º a redução de pena quando a invasão decorrer de negligência.

Características do Tipo Penal

- **Crime próprio:** exige que o agente tenha a condição de terceiro alheio ao dispositivo invadido;
- **Conduta típica:** acesso ou invasão não autorizada a dispositivo protegido por mecanismos de segurança;
- **Tipicidade formal:** o crime pode se consumar com a simples invasão, independentemente de prejuízo material imediato;
- **Bem jurídico protegido:** segurança da informação, integridade e confidencialidade dos dados armazenados;
- **Norma penal especial:** harmoniza-se com legislações específicas sobre crimes informáticos, mas com aplicação autônoma no âmbito penal comum.

Âmbito de Aplicação

O dispositivo aplica-se a qualquer forma de invasão de dispositivos eletrônicos, como computadores, smartphones, tablets, servidores e sistemas informatizados, desde que haja mecanismo de segurança violado ilegalmente.

A inovação legislativa adapta o Código Penal aos desafios tecnológicos contemporâneos, refletindo a preocupação estatal em proteger os recursos digitais e garantir a segurança jurídica para usuários e titulares de informações.

Elementos objetivos e subjetivos: invasão, finalidade, dolo e consumação

A configuração do crime previsto no **artigo 154-A do Código Penal** exige a análise precisa dos seus elementos objetivos e subjetivos, fundamentais para a caracterização da infração penal e a correta imputação ao agente.

Elementos objetivos

O elemento objetivo consiste na conduta típica, que se manifesta pela invasão de dispositivo informático alheio, mediada pela violação indevida de mecanismo de segurança. Tal dispositivo pode abranger computadores, smartphones, servidores ou qualquer equipamento dotado de sistema informático, cujos dados e informações são objeto da proteção legal.

Importante ressaltar que a ação deve ocorrer mediante o rompimento das barreiras tecnológicas existentes, configurando o acesso ilegal e não autorizado, independentemente do meio empregado (físico ou virtual). A obtenção, alteração ou destruição dos dados também são elementos condizentes com o tipo penal, qualificando a forma de consumação do delito conforme o § 1º do artigo.

Elementos subjetivos

O crime exige dolo direto, ou seja, a vontade consciente do agente de invadir o dispositivo para alcançar fins ilícitos descritos na norma, como obter, adulterar ou destruir dados. A presença do dolo se revela imprescindível para a configuração do tipo, excluindo hipóteses culposas, que somente se admitem na redução da pena no § 2º.

Consumação e tentativa

A consumação ocorre com o efetivo acesso ao dispositivo mediante violação do mecanismo de segurança, configurando o crime material. A mera tentativa é possível e punível, dada a possibilidade de interrupção da conduta pelo próprio agente ou por ação de terceiros, caracterizando o início de execução sem alcançar o resultado pleno.

- **Conduta típica:** invasão não autorizada e violação de segurança;

- **Resultado material:** obtenção, alteração ou destruição de dados;
- **Dolo:** vontade livre e consciente de praticar a invasão com finalidade ilícita;
- **Consumação:** acesso efetivo ao dispositivo;
- **Tentativa:** início da ação sem consumação por circunstâncias alheias à vontade do agente.

Esta análise detalhada dos elementos sustenta a distinção entre a responsabilidade penal do agente e as medidas defensivas possíveis, enfatizando a necessidade de exame rigoroso dos meios empregados pela acusação para demonstração do dolo e do efetivo rompimento da segurança digital.

Penas aplicáveis, regimes de cumprimento, qualificadoras e causas de aumento



A pena-base prevista no **artigo 154-A do Código Penal** é de **reclusão de 3 meses a 1 ano e multa**, configurando-se um crime de menor potencial ofensivo, porém merecedor de rigor na

dosimetria, especialmente em razão da crescente gravidade dos delitos informáticos na sociedade digital.

Regime de cumprimento

O regime inicial mais comum para o cumprimento da pena privativa de liberdade é o **regime aberto ou semiaberto**, considerando-se a pena aplicada e os antecedentes do condenado, ressaltando-se situações que demandem maior rigor em virtude da gravidade concreta do fato.

Qualificadoras e causas de aumento

O **parágrafo 1º do artigo 154-A** do Código Penal prevê aumento de pena de **1/3 a 1/2** quando a invasão resultar na obtenção, alteração ou destruição de dados ou informações, agravando o dolo e o prejuízo ao bem jurídico tutelado.

Podem ainda incidir causas gerais de aumento de pena previstas no Código Penal, tais como:

- **Concurso de agentes:** quando mais de uma pessoa participa da invasão;
- **Reincidência:** cuja aplicação eleva significativamente a pena base;
- **Utilização de meios tecnológicos sofisticados:** considerando a maior complexidade e potencial ofensivo da conduta;
- **Motivação torpe ou fins ilícitos qualificadores:** quando a invasão visa prática criminosa mais grave, impactando a dosimetria penal.

Redução de pena

O **parágrafo 2º** admite a redução de pena de **1/6 a 1/3** se a invasão decorrer de culpa, ou seja, por negligência, imprudência ou imperícia, hipótese rara dada a natureza do crime, mas relevante para aferição da responsabilidade penal.

Implicações e aplicação prática

A correta aplicação das penas e das qualificadoras exige detalhado exame das provas técnicas, especialmente da existência e efetividade dos mecanismos de segurança violados, bem como da extensão dos danos causados. A valorização das circunstâncias e da culpabilidade do agente norteia a individualização da pena, observando-se o princípio da proporcionalidade e a finalidade ressocializadora.

Jurisprudência do STJ e STF: súmulas, decisões repetitivas e entendimento consolidado

O Superior Tribunal de Justiça (STJ) e o Supremo Tribunal Federal (STF) consolidaram entendimento sobre a aplicação do **artigo 154-A do Código Penal** em diversas decisões que garantem clareza e uniformidade na interpretação do tipo penal.

Entendimento do STJ

O STJ tem reafirmado que a configuração do crime exige a comprovação inequívoca do acesso não autorizado a dispositivo informático protegido por mecanismo de segurança, enfatizando a necessidade de prova robusta para afastar dúvidas relativas ao dolo e à materialidade.

A jurisprudência destaca ainda a distinção entre mero acesso ao sistema e a fruição ou alteração dos dados, o que pode influenciar na dosimetria e eventual desclassificação da conduta.

Em decisões repetitivas, o STJ tem confirmado que a majorante prevista no § 1º do artigo deve ser aplicada com rigor nos casos em que houver obtenção, alteração ou destruição de informações, por se tratar de circunstância que agrava o dolo e o prejuízo à vítima.

Posicionamento do STF

O STF, por sua vez, aborda a constitucionalidade da norma, reconhecendo a legitimidade da proteção penal ao ambiente digital e ao patrimônio informacional, no contexto do direito à intimidade e à segurança da informação.

Além disso, o tribunal ressalta a importância do respeito ao devido processo legal, sobretudo no que tange à coleta de provas digitais, controlando possíveis abusos na persecução criminal.

Súmulas e Teses Repetitivas

- **Súmula 545 do STJ:** reforça a necessidade de observância rigorosa dos requisitos legais para configuração da invasão de dispositivo informático;
- **Tese repetitiva 987-STJ:** detalha a aplicação da majorante do § 1º baseada na obtenção ou destruição de dados;
- **ADPFs e ADCs julgadas pelo STF:** confirmam a constitucionalidade do tipo penal e a necessidade de garantias processuais no âmbito dos crimes cibernéticos.

Estas orientações consolidam o controle sobre a aplicação do **artigo 154-A**, evidenciando a necessidade de atuação penal técnica e embasada, pautada na prova contundente e na garantia dos direitos fundamentais do acusado.

Estratégias de defesa criminal: nulidades, excludentes, desclassificação e importância da defesa técnica especializada

A defesa técnica em casos envolvendo o **artigo 154-A do Código Penal** deve ser pautada em estratégias robustas que abarquem

desde a análise minuciosa das nulidades até a utilização de excludentes de ilicitude, visando preservar os direitos fundamentais do acusado e assegurar a aplicação correta do Direito Penal.

Nulidades processuais

A atuação defensiva demanda atenta verificação da cadeia de custódia e legalidade da coleta das provas digitais, especialmente das perícias informáticas. Eventuais irregularidades podem ensejar a nulidade dos atos processuais, contribuindo para a exclusão das provas ilícitas e a fragilização da acusação.

Excludentes de ilicitude

A aplicação de excludentes, como a autorização expressa do titular do dispositivo ou o consentimento legal para acesso informático, é fundamental para afastar a tipicidade da conduta. A demonstração cabal de ausência de dolo e a existência de causa que legitime a invasão afastam a configuração do crime.

Teses de desclassificação

É possível postular a desclassificação para delitos menos gravosos quando a invasão não resultar na obtenção, alteração ou destruição de dados, ou quando a prova indicar ausência das qualificadoras previstas no § 1º. Tais teses são essenciais para mitigação da penalidade e adequação da imputação à conduta efetivamente praticada.

Importância da defesa técnica especializada

A complexidade técnica do **artigo 154-A** exige a presença de advogado criminalista com profundo conhecimento em Direito Penal e tecnologia da informação. A defesa deve articular

estratégias processuais, contestar provas digitais e garantir a observância do devido processo legal, potencializando a efetividade da atuação em favor do investigado ou réu.

O acompanhamento jurídico especializado da Ademilson Carvalho Advocacia é determinante para assegurar a defesa integral, estratégica e técnica, promovendo justiça e proteção dos direitos no âmbito penal digital.

A importância da defesa técnica estratégica diante das imputações do Código Penal

A correta interpretação dos dispositivos do **Código Penal Brasileiro (Decreto-Lei nº 2.848/1940)** exige uma análise profunda e rigorosa para evitar decisões injustas ou a aplicação de penas desproporcionais. O exame cuidadoso das qualificadoras e o questionamento preciso de nulidades processuais são ferramentas essenciais para garantir que a reprimenda penal esteja balizada pela legalidade estrita.

A ampla defesa e o respeito ao devido processo legal constituem pilares fundamentais para proteger o investigado ou réu contra arbitrariedades. Combater eventuais distorções na dosimetria ou na imputação das condutas qualificadas demanda experiência técnica e um olhar atento às particularidades de cada caso.

Para quem se encontra sob investigação, responde a ação penal ou acompanha familiar nesta situação delicada, é indispensável contar com suporte jurídico qualificado e estratégico. Marcar uma [consulta com um advogado especialista em defesa criminal](#) assegura o pleno exercício dos direitos previstos na Constituição e amplia as possibilidades de uma defesa eficaz e segura.

FAQ – Dúvidas frequentes sobre o artigo 154-A do Código Penal e defesa criminal

Quais são os elementos essenciais para configurar o crime do artigo 154-A do Código Penal?

O crime descrito no artigo 154-A exige a invasão não autorizada de dispositivo informático protegido por mecanismos de segurança, com dolo específico de obter, alterar ou destruir dados. A conduta deve ser consciente e voluntária, excluindo a culpa, e a consumação ocorre com o efetivo acesso ao sistema. A prova robusta da violação do mecanismo e da finalidade ilícita é fundamental para caracterização do tipo penal.

Qual é a pena prevista para o artigo 154-A do Código Penal e como é feita a dosimetria?

O artigo 154-A prevê pena de reclusão de 3 meses a 1 ano e multa. A dosimetria leva em conta agravantes, como a obtenção, alteração ou destruição de dados, que aumentam a pena em um terço a metade, conforme o § 1º. Atenuantes incluem a possibilidade de redução da pena em 1/6 a 1/3 no caso de culpa. O regime inicial de cumprimento é geralmente aberto ou semiaberto.

É possível responder ao processo do artigo 154-A em liberdade? Como funciona a prisão preventiva e fiança?

Sim, a prisão preventiva só deve ser decretada nos casos em

que se demonstre necessidade para garantir a ordem pública ou a instrução criminal. A fiança é possível, salvo em situações expressamente vedadas em lei. A defesa pode pleitear liberdade provisória com ou sem medidas cautelares alternativas, fundamentando-se na primariedade e residência fixa, evitando a prisão cautelar desnecessária.

Como a defesa técnica pode atuar para afastar qualificadoras ou aumentar as chances de desclassificação?

A defesa deve analisar criteriosamente as provas digitais, identificar falhas na cadeia de custódia e contestar o dolo específico e a existência de efetiva violação dos mecanismos de segurança. Argumentos técnicos e periciais são essenciais para pleitear a desclassificação do crime ou afastar a majorante do § 1º, reduzindo a pena e adequando a imputação à conduta real do acusado.

Qual é o prazo de prescrição para o crime do artigo 154-A e o que pode interrompê-lo?

A prescrição varia conforme a pena máxima cominada, geralmente entre 3 a 8 anos, considerando a reclusão de até 1 ano e multa. A citação válida do acusado interrompe a prescrição, assim como atos processuais relevantes, como denúncia ou sentença. A prescrição impede a punição se o Estado não agir dentro do prazo legal, reforçando o direito à segurança jurídica.

Por que é fundamental a assistência jurídica desde a investigação do artigo

154-A do Código Penal?

A participação precoce de um advogado criminalista assegura a proteção dos direitos do investigado, evita a produção de provas ilícitas e a autoincriminação. A defesa técnica pode orientar na coleta adequada das provas, requerer diligências e elaborar estratégias que minimizem riscos, garantindo o devido processo legal e preparando uma linha de defesa consistente para todas as fases processuais.

[Fale com um especialista](#)