

Roteiro Jurídico Simplificado para Recuperação de Valores em Casos de Crimes Virtuais

Este roteiro foi elaborado para guiar vítimas de crimes virtuais na **recuperação de valores** de forma clara e eficiente. Baseado nas leis brasileiras, como o Marco Civil da Internet (Lei nº 12.965/2014) e a Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018), ele detalha os passos essenciais para proteger seus direitos e otimizar a investigação.

1. Registro Imediato do Boletim de Ocorrência (B.O.)

Ao ser vítima de um crime virtual, a **primeira e mais crucial ação** é registrar um Boletim de Ocorrência. Este documento oficial é a base para todas as etapas subsequentes e deve ser o mais detalhado possível.

O que incluir no B.O.: * **Descrição detalhada dos fatos:** Como o crime ocorreu, datas, horários e quaisquer interações. * **Evidências:** Anexe capturas de tela (prints), extratos bancários, comprovantes de transação, e-mails, mensagens e outros registros eletrônicos. * **Dados de identificação:** Forneça todos os dados relevantes dos envolvidos e das ferramentas utilizadas, como: * Números de telefone e WhatsApp. * Perfis de redes sociais. * Contas bancárias e chaves PIX envolvidas. * Endereços de e-mail. * Registros de data e hora das interações.



\n

2. Comunicação Urgente à Instituição Financeira

Após o registro do B.O., entre em contato **imediatamente** com o banco ou instituição financeira envolvida. Eles têm o dever de cooperar e garantir a segurança das transações.

O que solicitar ao banco: * **Bloqueio/Rastreamento de valores:** Peça o bloqueio ou rastreamento dos valores transferidos indevidamente. * **Extrato detalhado da conta:** Solicite um extrato completo da conta envolvida na fraude. * **Registros técnicos de acesso:** Requeira informações como endereços IP, identificadores de dispositivos (IMEI), navegador utilizado e outros dados técnicos relacionados ao acesso à conta. * **Dados das contas receptoras:** Obtenha os dados das contas para as quais os valores foram enviados.



\n

3. Exercício do Direito de Acesso a Dados (Judicialmente, se Necessário)

Caso a instituição financeira se recuse a fornecer as informações solicitadas, a vítima, por meio de um advogado, pode requerer judicialmente esses dados. Este direito é amparado por leis específicas:

- **Marco Civil da Internet (Lei nº 12.965/2014):** Art. 7º, incisos III e VI, que garantem o acesso a dados pessoais, registros de conexão e acesso a aplicações.
- **Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018):** Art. 18, inciso V, que assegura o direito do titular ao acesso facilitado aos seus dados pessoais.



Confirmação de que existe um ou mais tratamentos de dados sendo realizados



Acesso aos dados pessoais conservados que lhe digam respeito



Correção de dados pessoais incompletos, inexatos ou desatualizados



Eliminação de dados pessoais desnecessários, excessivos ou caso o seu tratamento seja ilícito



Portabilidade de dados a outro fornecedor de serviço ou produto, observados os segredos comercial e industrial



Eliminação de dados (exceto quando o tratamento é legal, mesmo que sem o consentimento do titular)



Informação sobre compartilhamento de seus dados com entes públicos e privados, caso isso exista



Informação sobre o não consentimento, ou seja, sobre a opção de não autorizar o tratamento e as consequências da negativa



Revogação do consentimento, nos termos da lei



Reclamação contra o controlador dos dados junto à autoridade nacional



Oposição, caso discorde de um tratamento feito sem seu consentimento e o considere irregular

\n

4. Requisição de Dados a Terceiros (Provedores e Plataformas)

Com base nos elementos coletados (telefones, e-mails, perfis de redes sociais, endereços IP, etc.), é fundamental solicitar dados a outras entidades, como plataformas digitais, empresas de telefonia e provedores de internet.

Idealmente, essa requisição deve ser feita pela **autoridade policial ou Ministério Público**. No entanto, em casos de demora ou omissão, o advogado pode buscar uma **ordem judicial específica** para obter esses dados. É importante ressaltar que este pedido não se confunde com interceptação telefônica, pois se refere a dados já armazenados (dados estáticos).

Consulta Requisição - Serviço de Terceiros

Consulta Manutenção

Requisição	Data da Requisição	Data Aprovação/Reprovação	Valor de Venda R\$ (866)
52	14/01/2022 11:50:44	14/01/2022 13:35:15	60,00
Nro O.S.	Descrição do Serviço	Valor de Custo R\$ (866)	
74769	3 - PINTURA	35,90	
Fornecedor (Fornecedores de Serviço de Terceiro) (867):			Nro/Serie Nota Fiscal Despesa Vinculada
14097	CLIENTE 2 - SERVIÇO TERCEIRO	123456	123
Usuário Solicitante	Observação da Requisição		
81 MELLO	teste		
Usuário Aprovador (848)	Observação do Aprovador		
13 CNP			
Situação: Nota Faturada			
Aprovar (848)		Reprovar (848)	
Reabrir (865)		Imprimir (868)	
		Gravar	
		Cancelar	

\n

5. Pedido de Preservação de Dados

Para garantir a integridade das informações e evitar que sejam apagadas, é altamente recomendável solicitar, de forma preventiva, a **preservação dos dados** relacionados ao crime. Este pedido deve ser direcionado às plataformas e provedores envolvidos, com base no Art. 13 do Marco Civil da Internet.

Esta medida assegura que as evidências digitais permaneçam intactas até a conclusão das investigações policiais ou decisão judicial.



\n

Conclusão

A **ação rápida e coordenada** entre a vítima, as autoridades e as instituições financeiras, amparada pela legislação vigente, é essencial. Seguir este roteiro aumenta significativamente as chances de sucesso na investigação criminal e na recuperação dos valores subtraídos, ao mesmo tempo em que protege os direitos da vítima.

Mapa Mental: Roteiro para Recuperação de Valores em Crimes Virtuais

