Modulações de Transparência em Organizações Privadas: Disputas de sentido durante instabilidades do jogo *League of Legends*[1]

Fernanda Shelda de Andrade Melo[2]

Resumo

O tema da transparência em organizações privadas vem ganhando espaço nos últimos anos. Neste trabalho, propomos unir essa discussão junto às lógicas adaptadas pelos jogos eletrônicos durante períodos de instabilidade, como é o caso dos ataques cibernéticos. Dessa forma, verificamos a importância de entender como as organizações trabalham lógicas de transparência enquanto estão vulneráveis. O objetivo foi delimitado em identificar as modulações de transparência durante o ataque cibernético direcionado ao jogo *League of Legends*, contrastando possíveis disputas de sentido entre públicos e organização ao longo desse período. Para atingi-lo, utilizamos a metodologia exploratória baseando o conteúdo em uma análise dimensional. Os resultados apontaram uma vertente interessante de transparência, em que primeiro é adotado um sistema de invisibilidade e, em um segundo momento, a organização lança relatórios sobre o acontecimento.

Palavras-chave

Transparência; comunicação organizacional; jogos eletrônicos.

Introdução

A palavra transparência pode ter diferentes significados na ciência a depender da abordagem contextual. Por exemplo, na física a transparência pode estar ligada ao estudo de materiais, enquanto na química pode implicar uma lógica de limpeza. No geral, o termo está relacionado à ideia de abertura, permitindo que algo ou alguém possa ser visto, contrariando a opacidade. No âmbito das abordagens acadêmicas da ciência política que cercam práticas governamentais, a transparência é uma condição consolidada como indispensável para a democracia e que é responsável pelo incentivo da participação pública nos diversos moldes de governabilidade (Gomes, 2017; Silva, 2016).

Nos últimos anos, novas discussões envolvendo a lógica da transparência estão surgindo nas diversas áreas do conhecimento. Isso inclui os estudos organizacionais, a partir do destaque para o termo "transparência empresarial" (Vieira, 2015). Difundida à priori nos debates da administração, podemos considerar que a transparência também está fortemente ligada ao

[1] Trabalho apresentado na modalidade Comunicações Livres, atividade integrante do XVIII Congresso Brasileiro Científico de Comunicação Organizacional e de Relações Públicas.
[2] Doutoranda do Programa de Pós-Graduação em Comunicação Social da Universidade Federal de Minas Gerais (UFMG). E-mail: contatofernandaandrade@hotmail.com.

âmbito comunicativo das organizações, já que participação dos diversos públicos, tanto na tomada de decisões como no processo de abertura informacional dessas empresas, é uma relação indispensável para ambos. No caso das organizações, há a construção de um vínculo de confiança com seus possíveis clientes, enquanto no caso dos públicos, é uma forma de participar e entender como funcionam as empresas das quais consomem, afinal, "a transparência tem inerente a caraterística da divulgação de informação e isto permite aos consumidores agirem mais planeada e ponderadamente, contribuindo para um aumento do seu poder negocial e possibilitando-lhes realizar escolhas mais conscientes" (Dias, 2016, p. 3).

Por vezes, a cobrança por transparência nas organizações se intensifica quando há uma instabilidade ou maior descrédito. Revisitando a transparência aplicada nos governos, o processo de instabilidade política pode incentivar levantes que cobrem justamente por maior abertura dos processos (Vello, 2017). Algo semelhante pode acontecer nas organizações privadas e um forte exemplo disso está nos ataques cibernéticos: anteriormente associados ao famoso termo de invasão *hacker*, os ataques podem ter diversos objetivos que envolvem a quebra de segurança dos sistemas de uma empresa, incluindo o roubo de dados (Araujo; Rossi, 2020). Neste caso, os públicos podem ou não saber do ataque e se tornam vulneráveis (juntamente das organizações), já que as informações sensíveis deles – como dados de cartões de crédito, cadastros pessoais e afins – podem ser vazados.

Em 2023, o jogo *League of Legends*, sediado pela empresa Riot Games, sofreu um desses ataques. Durante a ação, os invasores pediram um valor monetário de resgate para que não vazassem o código roubado. Esse contexto, porém, só foi divulgado pela organização após dias de vários processos de instabilidade notados pelos jogadores, marcando uma disputa de sentidos entre o que era relatado e cobrado pelos consumidores e aquilo que veio – ou deixou de vir – à público por uma tomada de decisão da organização.

Verificamos uma vertente interessante de pesquisa neste artigo, pois além de nutrir os assuntos discutidos acima relacionando a transparência organizacional no quesito dos ataques cibernéticos, podemos ainda identificar como empresas ligadas aos jogos, em que as instabilidades podem ser mais perceptíveis porque atacam diretamente a jogabilidade em tempo real dos usuários, podem criar suas próprias lógicas de transparência durante a elaboração de estratégias comunicativas. Além disso, a Riot Games é conhecida por propor ferramentas de transparência para os seus jogos e atua com uma construção discursiva baseada em quesitos de

abertura e de participação de seus lançamentos, manutenções do jogo e modificações que aparecem em seus relatórios anuais, incluindo levantamentos de impactos na sociedade[3].

Isso significa que o presente artigo propõe entender como uma empresa de jogos que constrói uma lógica discursiva baseada na utilização da transparência com seus consumidores pode se mobilizar quando é alvo de um ataque, abrindo margem para uma espécie de escolha entre adotar ou não adotar medidas de transparência a depender do contexto da organização. Nesse sentido, o objetivo geral deste trabalho foi definido em identificar as modulações de transparência durante o ataque cibernético direcionado ao jogo *League of Legends*, contrastando possíveis disputas de sentido entre públicos e organização ao longo desse período.

Para atingir tal meta, consideramos duas etapas metodológicas, iniciando com uma pesquisa bibliográfica para entender as principais teorias e bases do assunto discutido, partindo para uma fase analítica que está centrada em uma pesquisa exploratória que categoriza duas dimensões de análise: a organização comunicada e a organização comunicante. Neste caso, foi possível perceber as posições adotadas pela Riot Games durante o contexto citado, além da interação de seus jogadores no mesmo período dentro da rede social X (antigo Twitter)[4]. Os resultados principais apontam para a utilização da opacidade durante os primeiros momentos do ataque, o que gerou disputas entre públicos e organização sobre o motivo das instabilidades, partindo para uma tentativa de relatar o acontecimento de forma detalhada posteriormente.

O que é a transparência em organizações privadas?

Quando falamos em transparência de informações, o imaginário social pode acionar a lógica democrática, como citado anteriormente. Apesar de serem aplicadas de formas distintas, o sentido da transparência continua sendo o mesmo. Na vertente política, o acesso de informações é um direito evidenciado desde a Constituição Federal de 1988 no artigo 5º, e esse direito ganhou ainda mais força após a elaboração da Lei de Acesso à Informação (LAI) em 2011. Dessa forma, todos os municípios e estados com mais de 10 mil habitantes são obrigados a publicar dados sobre o funcionamento da sua gestão, como é o caso de remuneração, gastos com obras, projetos em andamento e afins.

Porém, voltando o olhar para as organizações privadas, esse cenário é bem diferente. Não há nenhuma obrigação de compartilhar informações sobre a empresa, ressalvo os casos em que elas estão ligadas a financiamentos públicos – como é o caso das licitações governamentais.

[3] Relatório de Impacto de 2022 Riot Games. Disponível em: https://www.riotgames.com/pt-br/2022-riot-games-impact-report. Acesso em 19 fevereiro 2024.
[4] X (Twitter). Disponível em: https://twitter.com/home. Acesso em 21 fevereiro 2024.

Fora disso, a tomada de decisão de se tornar transparente é exclusivamente da organização. Para além disso, por vezes, essa lógica é utilizada na captação e manutenção de investidores e, nesses casos, há um compartilhamento de dados específicos que mostrem benefícios no patrimônio daquela companhia. Isso significa que, além de não ser direcionado ao público, esse exemplo mostra um trabalho de recorte das informações, nutridos pelo interesse monetário. Um forte exemplo deste caso está no ataque cibernético da empresa Renner[5], em 2021, que enquanto sofria com instabilidades divulgou o primeiro comunicado do acontecimento para seus investidores, utilizando inclusive uma aba específica do site para *stakeholders*. Somente após isso, as informações foram repassadas de forma mais lenta para clientes.

Por isso, é importante destacar que quando citamos a transparência organizacional queremos relacionar esse compartilhamento com os públicos e não necessariamente com *stakeholders* e colaboradores. Essa é uma ideia primária da transparência empresarial, trabalhada por autores como Rincón (2020) que defende o repasse honesto de informações e abertura participativa para os funcionários dessas organizações. Concordamos que essa é uma prática indispensável para o bom funcionamento da empresa, mas adicionamos um novo olhar: a necessidade de que essas informações e contrastes também cheguem ao público externo.

Para Silva (2022) a transparência pode ser usada como uma ferramenta para favorecer uma unidade do corpo empresarial e, dessa forma, a criação de redes de informação poderia implicar no contraste ético da empresa, evidenciando boas práticas. Além disso, Williams (2005) destaca que a transparência tem uma forte relação com a ideia de confiança, tornando-se um precedente para uma boa relação dos públicos com tais organizações.

Vale reiterar que não estamos propondo um vazamento de todas as informações da organização, como é o caso de estratégias e dados sensíveis, mas sim uma prática que permita maior participação dos públicos e, para além, possa indicar o funcionamento da empresa, norteando suas condutas e minimizando as vulnerabilidades dos públicos em situações de crise. Citamos, por exemplo, o contexto dos ataques cibernéticos, momento em que as organizações são alvo de criminosos que tentam invadir os sistemas e "sequestrar" possíveis informações sensíveis ou até mesmo divulgá-las. Além da vulnerabilidade das empresas, por estarem à mercê da situação, a sociedade também se torna vulnerável, pois são dados como cartões e documentos, como o Cadastro de Pessoa Física (CPF) e o Registro Geral (RG), que podem ser vazados sem que os clientes sequer saibam que isso está acontecendo – caso não seja informado pela empresa.

[5] Site da Renner sai do ar após ataque hacker – entenda o caso. CNN Brasil, 2021. Disponível em: https://encurtador.com.br/mWX36/. Acesso em 21 fevereiro 2024.

Com ações mais participativas é ainda possível evidenciar um *accountability*. Este termo está ligado à responsabilização das organizações quando um problema pode atingir os públicos, e para Cunha Filho (2018) é um resultado da transparência de acordo com a fórmula T > P > A, em que T é transparência, P é a participação dos públicos neste processo, e A a possível responsabilização gerada neste processo. O compartilhamento de informações ainda pode "reduzir a possibilidade de omissão entre os dados dos processos, possibilitar o controle sobre os produtos e serviços prestados, facilitar a investigação, e aumentar a confiança entre as organizações e a sociedade" (Aló, 2009, p. 19). Por isso, entendemos que a utilização das estratégias que possam nortear a divulgação de informações na adaptação de uma empresa cada vez mais transparente favorece não só a perspectiva dos públicos, mas a própria organização.

Como esse cenário funciona nos jogos

Para compreender como a discussão anterior pode ser aplicada nos jogos e, principalmente, no contexto das instabilidades e ataques, é preciso revisitar algumas lógicas básicas aplicadas em organizações responsáveis pelos *games*. Tais sistemas geralmente são subsidiados por empresas que separam categorizações a depender do tipo do jogo, que são variáveis. Por exemplo, a Eletronic Arts (EA) é, ao mesmo tempo, responsável pelo jogo *Fifa* – famoso entre o segmento de futebol – e pelo jogo *The Sims*, plataforma de realidade aumentada social que pouco tem a ver com o tema esportivo do primeiro exemplo.

Neste caso, estamos trabalhando com a lógica dos jogos digitais: "A existência de mundos fictícios é a principal característica que distingue os jogos digitais dos não-digitais, que por sua vez são essencialmente abstratos. É importante ressaltar que a existência de mundos fictícios deve-se a existência de um mundo lúdico único onde o jogo se desenvolve" (Lucchese; Ribeiro, 2009, p. 7) Uma funcionalidade muito abordada pelas organizações que cuidam desse segmento está na relação de ganhar algo. Isto é, quanto mais metas os usuários têm a atingir e desafios mais difíceis, mais presos eles ficam ao condicionamento de jogar constantemente.

Outra coisa importante é que quando os jogos lidam com a necessidade de habilidade, o consumidor pode cada vez mais ganhar confiança em si mesmo e, consequentemente, sentir-se no controle do personagem e de toda a situação (Campos, 2022). Podemos usar o exemplo do jogo citado Fifa: para controlar um personagem que representa um jogador de futebol, o usuário precisa, cada vez mais, entender das habilidades daquela figura específica; dos controles que são utilizados como funcionalidade para controlar o boneco; e de técnicas cada vez mais elaboradas para levá-lo a cumprir o objetivo: fazer o gol.

Mas, afinal, chegamos ao primeiro questionamento deste tópico: por que aplicar transparência organizacional em um jogo? Para chegar a uma resposta precisamos considerar que qualquer mudança ínfima em um sistema afeta diretamente um usuário. A mudança da cor de um botão, por exemplo, pode fazer com que ele seja mais ou menos clicável de acordo com a lógica do *design thinking* (Martins Filho *et al.*, 2015). Isso serve para outros aspectos dos *games*, como mudanças de ferramentas, habilidades dos personagens e atualizações diversas. Esse cenário ainda pode pontuar maior participação dos usuários no jogo, como indicar melhorias e participar dos processos criativos de acordo com a sua experiência.

Vale considerar ainda que os jogos não só ficam na esfera do entretenimento gratuito, mas boa parte deles envolve um quesito monetário. Alguns precisam ser comprados antes de jogar (como é o caso dos exemplos da Eletronic Arts), enquanto outros – como o *League of Legends* – não precisam ser comprados e o acesso é livre, mas oferecem diversas funcionalidades dentro da aplicação que podem ser adquiridas. Esse é o caso da personalização dos bonecos, de melhorias para a experiência do jogador e até pagamento para modificar o nome de avatar. Ou seja, um possível vazamento de dados na perspectiva dos ataques cibernéticos poderia afetar a quebra de sigilo de cartões e outros dados relacionados à compra.

Chegamos então à segunda indagação: como acontecem esses ataques cibernéticos quando o alvo são jogos? No Brasil, os dois ataques mais comuns são conhecidos como *ramsoware* e *DDoS*. Este último está ligado à interferência dos sistemas, como o envio de muitas requisições ao mesmo tempo que podem deixar os sites lentos. Ele não provoca especificamente um interrompimento do sistema, mas sim uma superlotação e seu objetivo é prejudicar a experiência do usuário que acessará esse serviço. Enquanto isso, o *ramsoware* é o mais grave. É quando os criminosos conseguem acessar bases de dados da ferramenta, vazá-las para utilizar dessas informações ou até pedir um valor para resgate, já que no meio desse "rapto" das informações as empresas podem perder dados importantes para a continuidade dos serviços (Araujo; Rossi, 2020).

Isso significa que quando falamos dos jogos, precisamos identificar que esses sistemas podem ser, inclusive, copiados ou fraudados. É o que pode ser chamado de *script*, quando alguém descobre uma falha no código do jogo e então lança alguma ferramenta para abusar desse erro obtendo vantagens. Outro cenário é o próprio alcance de informações pessoais dos jogadores que envolve uma vulnerabilidade preocupante quanto à possibilidade de uma grande afetação na vida dessas vítimas.

Esse contexto demonstra como as organizações precisam parar de pensar na *ciber* segurança apenas em um modelo empresarial, preocupando-se essencialmente com os lucros

na perspectiva dos *stakeholders* e entender que a imagem e a responsabilidade com os clientes também são categorias afetadas durante essas crises (Walters, 2015). É preciso seguir bons exemplos, como é o caso da Microsoft que informou os clientes de uma brecha no sistema em 2017, disponibilizando dois dias após o ataque uma atualização que pudesse proteger os usuários – todos os passos e possíveis danos informados pela empresa durante o período de ataque (Lima, 2017). Comunicar também é amparar os clientes que se encontram em uma posição vulnerável tanto quanto a empresa nestes momentos e, consequentemente, minimizar possíveis danos.

Fase analítica

O jogo alvo de estudo deste trabalho está enquadrado como digital. *League of Legends* foi lançado em outubro de 2009 pela Riot Games em um modo multijogador – os usuários podem jogar contra robôs ou contra outros jogadores. O objetivo principal de uma partida normal é destruir as torres do time inimigo e sua base. Para isso, cada jogador pode escolher um personagem que contém habilidades e especificidades diferentes e começar a luta com mais quatro pessoas. Essa lógica envolve a perspectiva discutida anteriormente, pois cada personagem possui um modelo de jogabilidade diferente, logo, exige uma maior especialização do jogador. Além disso, conta com diferentes níveis e rankings, contrastando a competitividade para que os usuários continuem acessando mais e mais.

Durante os últimos anos, a empresa subsidiária do LOL (sigla pela qual os jogadores chamam o *game*) vem tentando adotar um discurso baseado na transparência de suas práticas. Um forte exemplo está na restrição de chat. Por possuir um bate papo aberto entre os jogadores durante a partida, o LOL lidava com a responsabilidade de punir usuários que quebrassem regras e difamassem outras pessoas durante a partida. Em 2013, a Riot aplicou no jogo a restrição de chat, algo comum dentro das plataformas *multiplayer*. Dessa forma, infringir uma regra poderia levar o jogador à uma punição – como o *mute*, ato em que o usuário fica proibido de se comunicar durante um período de tempo específico, ou o banimento, quando o acesso ao jogo é totalmente vedado.

A inovação da Riot, no entanto, está no relato desse sistema de penalidades. Desde 2013, o processo passou por inovações para chegar no modelo atual em 2022, em que as mensagens exatas dos jogadores são identificadas automaticamente e exibidas no final da partida, explicando exatamente qual foi o erro do jogador e liberando o registro de chat (histórico/*log*). Apesar de parecer algo simples, a Riot é uma das poucas subsidiárias que aplicam essa ferramenta de forma mais transparente, pois outros *games* famosos – como é o caso do Fortnite

– aplicam a penalidade sem demonstrar registro do código do jogo para o usuário. Além disso, no LOL, o jogador ainda pode receber atualizações após realizar uma denúncia, entendendo como sua colaboração foi utilizada para melhorar a conduta dentro da plataforma.

Além disso, o processo de criação e modificação do jogo também segue uma perspectiva aberta ao público. Por exemplo, é comum que funcionários da organização forneçam declarações abertas à imprensa relatando novos projetos que contam com a participação do público e o que pode ou não ser modificado nessa perspectiva para que não haja expectativas fora daquilo que é aplicável[6]. Nas redes sociais, a conta do LOL (@LoLBR) frequentemente publica abertura de *feedbacks* e um processo detalhado dos projetos criativos. Esse é o caso do lançamento de novos personagens que podem ser observados passo a passo, desde a ideia até o desenho e o conceito. Os usuários podem, consequentemente, motivar uma opinião pública que resulte na modificação desses personagens. Esse caso aconteceu com a campeã Yuumi, após grande crítica dos jogadores na rede antes e durante seu lançamento. A personagem sofreu grandes modificações nas atualizações seguintes.

No entanto, neste trabalho, pretendemos verificar se essa lógica é adaptada durante o processo de instabilidades, principalmente quando a empresa também está passando por um momento de vulnerabilidade, como é o caso do ataque cibernético. Após as discussões apontadas nas seções teóricas, estruturamos a fase analítica em uma pesquisa exploratória. Escolhemos a rede social X – antigo Twitter – para verificar a disputa de sentidos entre os usuários e a conta oficial da organização. A escolha do X deve-se à grande interação permitida através dos *tweets*, além da Riot utilizar amplamente desta rede para declarações oficiais.

Foram aplicadas duas fases metodológicas. Na primeira, resgatamos materiais na rede social X a partir de um recorte temporário. No dia 20 de janeiro de 2023, a conta da Riot (@riotgames) revelou ter sofrido um ataque cibernético no começo daquela semana. Quatro dias depois, foi publicado na mesma conta um comunicado mais profundo sobre o ataque. Por isso, setorizamos os tweets que estivessem ligados à conta da empresa (@riotgames), do jogo (@LoLegendsBR) e aos nomes LOL e *League of Legends* durante o período de 10 a 25 de janeiro de 2023. Para isso, foi utilizada a fórmula “termos específicos (from: conta desejada) until:período máximo since: período mínimo”.

Após o alcance desse conteúdo, aplicamos a lógica de Bardin (2011) para obter uma contextualização do conteúdo resgatado. Para tal, foram separadas duas dimensões e seus

[6] Transparente, Riot aponta o que não vem gostando no Lol, ESPN, 2018. Disponível em: https://www.espn.com.br/esports/artigo/_/id/4625489/transparente-riot-aponta-o-que-nao-vem-gostando-no-lol-e-os-proximos-objetivos-com-as-mudancas-no-jogo. Acesso em 21 fevereiro 2024.

respectivos indicadores, baseando-se nas discussões da comunicação organizacional na perspectiva da complexidade (Baldissera, 2009). A primeira dimensão é a organização comunicada, tratando dos processos oficiais e comunicados da Riot Games. Enquanto isso, a segunda dimensão está ligada à organização comunicante, na visão dos usuários do jogo e suas interações na rede social, quando há possivelmente uma cobrança direcionada à organização ou uma via de interação que questiona o acontecimento, propondo "estabelecer relação com a organização. Além dos processos planejados, também assumem relevo os processos que se realizam na informalidade; inclusive aqueles que irrompem sem que a organização tenha conhecimento" (Baldissera, 2009, p. 118).

Vale pontuar que as dimensões não estão em uma ordem hierárquica de levantamento, mas servem para contextualizar a abordagem do conteúdo explorado. Isso porque alguns questionamentos e cobranças surgem antes mesmo dos comunicados e continuam após o posicionamento da organização, evidenciando que as disputas de sentido estão presentes a todo momento em ambas as dimensões (Tabela 1).

Tabela 1. Dimensões e indicadores da análise.

Dimensão		Indicador
I.	Organização Comunicada	Comunicados da empresa no X (tweets)
II.	Organização Comunicante	Questionamentos à empresa no X (tweets)

Fonte: Elaborado pela autora.

Ao iniciar a análise durante o levantamento dos *tweets* advindos do público na lógica da tabela acima, notamos uma grande quantidade de menção à instabilidade do jogo nesse período. A utilização comum era do termo "cair", pois quando o jogo "cai" ele está fora do ar. Nesse sentido, filtramos a separação dos *tweets* com a adição do termo cair e/ou caindo, resultando em 64 tweets relacionados à palavra no contexto da instabilidade do LOL. O pico dessas reclamações aconteceu entre o dia 14 e 15 de janeiro de 2023.

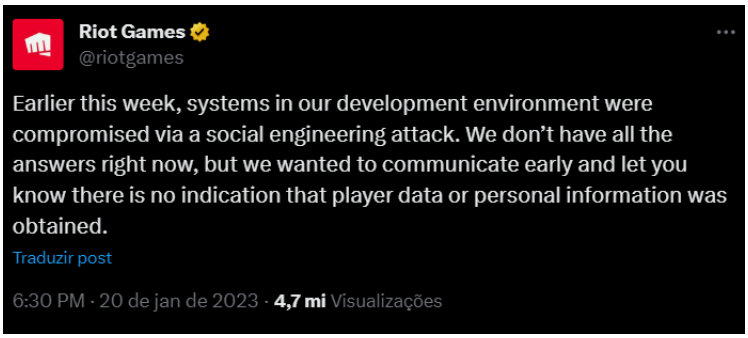
Figura 1. Publicações que questionam a instabilidade do jogo.

Fonte: Captura de tela realizada a partir do levantamento metodológico na rede social X (antigo Twitter).

Isso significa que até o momento dos *tweets* acima, o público não fazia ideia do que estava acontecendo, indicando que poderia ser uma questão de erro dentro do jogo. Alguns deles chegam a culpar a empresa e marcar o perfil oficial, outros tentam testar a própria internet para entender se o problema era individual ou no sistema. No material levantado também aparecem constantes reclamações que estão relacionadas aos *scripts*. *Scripts* é o termo utilizado para se referir aqueles que conseguem uma brecha no código do jogo e, consequentemente, desenvolvem ferramentas para adquirir vantagens e prejudicar outros avatares. Por exemplo, se o usuário precisa pressionar R + E para realizar uma função específica, um *script* pode elaborar um mecanismo para que essa função seja feita automaticamente, sem precisar pressionar. Isso encurta o tempo e favorece a jogabilidade. Como citado anteriormente, o aumento de *scripts* pode estar relacionado ao vazamento de dados que permite uma brecha na manipulação do código. As reclamações relacionadas aos *scripts* se concentram após o dia 18.

É apenas no dia 20 de janeiro de 2023 que notamos, então, um posicionamento da empresa que, nos dias antecedentes, não havia publicado nada em relação aos sistemas dos jogos, apenas atualizações padronizadas sobre personagens. No primeiro comunicado, a empresa começa dizendo que “No início desta semana, os sistemas do nosso ambiente de desenvolvimento foram comprometidos por meio de um ataque de engenharia social”, sendo este tipo de ataque uma espécie de manipulação e fraude para conseguir informações de acesso através de um colaborador. O *tweet* continua: “Não temos todas as respostas no momento, mas queremos comunicar antecipadamente e avisar que não há indícios de que dados ou informações pessoais dos jogadores foram obtidos” (Figura 2).

Figura 2. Primeiro comunicado da Riot Games sobre o ocorrido.

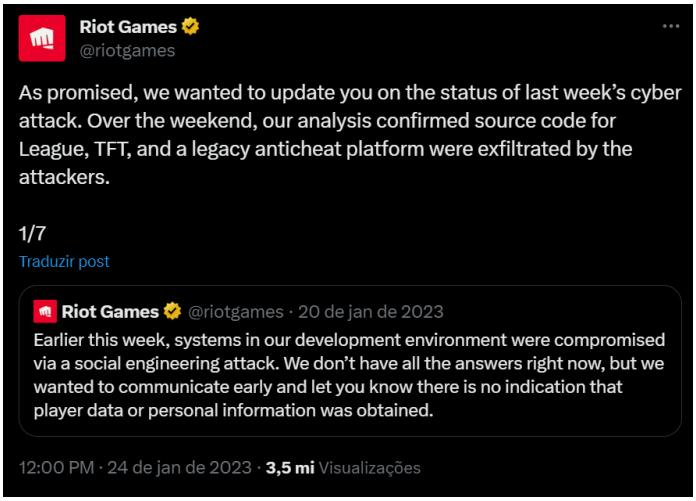


Fonte: Captura de tela realizada a partir do levantamento metodológico na rede social X (antigo Twitter).

Vale reiterar que procuramos a versão do comunicado publicada nas contas brasileiras da empresa – tanto representando a subsidiária, como o jogo – e não encontramos uma versão de publicação oficial traduzida. Os veículos de imprensa ligados ao segmento dos jogos foram responsáveis por transmitir os avisos em outras línguas, como no português. Esse raciocínio demonstra uma vulnerabilidade dos jogadores que não possuem a língua inglesa como primária e, consequentemente, dependem da atuação vigilante dos veículos midiáticos para fazer esse papel informativo.

Além disso, notamos que o dia aproximado indicado como alvo do ataque bate com os dias em que os jogadores estavam reclamando constantemente das instabilidades, uma vez que o comunicado foi publicado no dia 20 (uma sexta-feira) afirmando que aconteceu no início da semana – aproximadamente entre o dia 14 e 16 de janeiro. Essa correlação de instabilidades não é, no entanto, pontuada no comunicado, há apenas uma menção à inviabilidade de continuar novos lançamentos em um *tweet* seguinte. Somente depois de quatro dias, a Riot Games complementou o comunicado com uma versão atualizada desse caso (Figura 3).

Figura 3. Segundo comunicado da Riot Games sobre o ocorrido.



Fonte: Captura de tela realizada a partir do levantamento metodológico na rede social X (antigo Twitter).

Por meio de sete *tweets*, a empresa ressalta que a análise indicou onde estava o problema do vazamento e o que foi invadido. Segundo a organização, os criminosos responsáveis pelo ataque enviaram um e-mail para a Riot Games pedindo um valor monetário para não vazar o código acessado. Tal código estaria relacionado à fonte do jogo e às configurações das ferramentas, o que, portanto, poderia aumentar o número dos *scripts* citados anteriormente, afinal, agora poderiam criar novas fugas contendo informações mais completas sobre o funcionamento interno do *game*. Pontuamos aqui, novamente, a semelhança da afirmação com a reclamação anterior dos usuários em relação ao aumento de *scripts* que já tinha sido notado e questionado dias antes do comunicado.

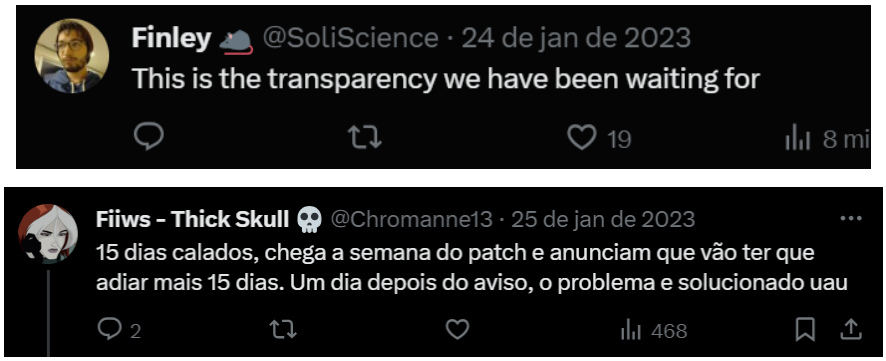
Nessa sequência, a Riot volta a enfatizar e garantir que nenhum dado pessoal teria sido acessado ou comprometido. Finalizam reiterando que as autoridades e a própria equipe investigarão de onde partiu o ataque para punir os responsáveis e proteger a plataforma para que não aconteça novamente. A Riot ainda pontua algo interessante ao final do comunicado: "Estamos comprometidos com a transparência e lançaremos um relatório completo no futuro detalhando as técnicas do ataque, as áreas em que a segurança da Riot falhou e os passos que estamos dando para garantir que isso não aconteça novamente". Assim como o primeiro comunicado, este também não foi encontrado em sua versão traduzida na conta brasileira.

Encontramos aqui alguns pontos interessantes. Até a completa identificação da invasão e divulgação de que isso estava acontecendo, os jogadores já tinham sentido os prejuízos deste ataque durante suas jogabilidades. Eles não imaginavam, *à priori*, que a causa seria algo bem mais grave que uma leve instabilidade. Nesse sentido, podemos considerar que os públicos ficaram vulneráveis durante dias – enquanto acontecia o ataque e, consequentemente, durante os quatro dias seguintes ao comunicado mais completo. O período de quatro dias, apesar de necessário para a finalização da investigação do que aconteceu, pode indicar um momento nebuloso no sentido informativo para os jogadores, causando uma onda de desinformação, dúvidas e boatos sobre o que realmente havia acontecido.

Esse raciocínio gerou diferentes opiniões a partir das respostas dos públicos para esses posicionamentos. Em certa perspectiva apontada na Figura 5, o usuário responde que “essa era a transparência pela qual esperamos”, indicando que o segundo comunicado pode ter adotado uma posição satisfatória em relação à transparência do caso. Enquanto isso, um jogador que aguardava a estreia de um novo *patch* – atualização do jogo com lançamentos inéditos que estava prevista para o mesmo período – contesta a quantidade de dias em silêncio durante as instabilidades. Sugerindo que o comunicado do ataque poderia ter sido usado como desculpa para adiar os lançamentos que não estavam prontos, ele afirma que após o segundo aviso o

patch teria sido aplicado normalmente, o que pode ter gerado um desencontro de ideias e dúvidas (Figura 5 e 6). Ambos os *tweets* advém de respostas do segundo comunicado publicado pela Riot.

Figura 5 e 6. Respostas de internautas ao segundo comunicado.



Fonte: Captura de tela realizada a partir do levantamento metodológico na rede social X (antigo Twitter).

Podemos afirmar que, durante este ataque, a Riot Games – representando o *League of Legends* – atuou com diversas modulações na prática da transparência empresarial. Isso porque, primeiramente, houve uma tentativa de invisibilidade – sem resposta para as reclamações das quedas constantes do sistema e falta de postagens durante o período de incertezas. A conta brasileira do jogo chegou a ficar mais de uma semana sem publicações durante o momento de cobrança dos públicos. Além disso, após o primeiro comunicado, há uma pausa de quatro dias sem novas informações e respostas sobre o caso. Nesse sentido, a empresa trabalhou com períodos de opacidade para construir estratégias sobre a situação. A adoção do sistema de invisibilidade é um mecanismo utilizado para que haja um breve esquecimento sobre o que está acontecendo: "Não ser mencionado, por vezes, passa a ser uma moeda valiosa quando os resultados decorrentes dessas referências/associações à organização acionam/despertam significação negativa" (Silva, 2018, p. 18).

Em seguida, notamos a tentativa de proceder um *accountability* (responsabilização) através da fórmula de Cunha Filho (2018) apresentada anteriormente, em que T > P > A. Notamos que a partir do primeiro comunicado, a pressão pública em relação aos questionamentos do que poderia ter acontecido pode ter forçado a posterior responsabilização em um formato mais completo. Neste caso, o primeiro posicionamento atuou no formato primário da transparência (T), incentivando a participação e cobrança dos públicos sobre o caso (P) e gerou a responsabilização de forma mais completa no segundo comunicado (A).

Evidenciamos também que, apesar das divergentes cobranças exemplificadas nas Figuras 5 e 6 sobre os resultados das publicações na opinião pública, a quantidade de *tweets*

como resposta ao segundo comunicado foi mais inclinada aos elogios à organização, enxergando o posicionamento mais completo como algo positivo. O termo transparência aparece diversas vezes nas menções deste comunicado, pontuando que o público pode ter entendido como uma boa intenção o aprofundamento das explicações. Esse cenário é divergente do primeiro comunicado mais curto, em que as respostas estão centradas em dúvidas e desconfiança sobre o ataque.

Encontramos, porém, algo interessante: não houve uma republicação com o relatório que é informado no final dos *tweets* sobre o detalhamento da invasão. Inclusive, alguns usuários voltaram à publicação para essa cobrança, como no caso a seguir em que o internauta questiona a empresa cinco meses após o ataque (em junho) e, posteriormente, nove meses após o ataque, em outubro: "esse relatório foi lançado?" (Figura 7).

Figura 7. Cobrança pelo relatório prometido pela Riot Games.

Fonte: Captura de tela realizada a partir do levantamento metodológico na rede social X (antigo Twitter).

Neste caso, a narrativa da transparência pode ter sido usada apenas como um sentido discursivo para gerar confiança e uma boa manutenção da relação da organização com os jogadores, deixando de lado os problemas práticos da instabilidade e do grande aparecimento dos *scripts*, algo que poderia ser minimizado com a divulgação das investigações. Além disso, o relatório, aparentemente, não foi compartilhado nas redes sociais e também não foi encontrado no site oficial, esperamos que esse levantamento possa ser lançado ainda em 2024, após completar um ano do ataque.

Considerações finais

O presente trabalho procurou discutir a transparência empresarial aplicada em um contexto de instabilidade, exemplificado no ataque cibernético sofrido pelo jogo *League of Legends*, contrastando não só as bases teóricas, mas também a lógica prática aplicada pela organização durante o incidente. Por isso, não propomos novos conceitos de transparência ou o que se norteia como certo e errado, mas sim entender as possibilidades estratégicas que visavam minimizar ou maximizar as vulnerabilidades, tanto das organizações como dos públicos neste período.

A partir da fase analítica, verificamos que a Riot Games de fato indicou uma tentativa de comportamento transparente ao relatar detalhadamente e assumir o ataque. Isso pode ser visto nos comunicados que dão ênfase na proteção dos dados dos usuários. No caso do segundo posicionamento, há ainda uma explicação de como o ataque ocorreu, incluindo as estratégias utilizadas pelos invasores para deixar claro como podem agir futuramente se defendendo de um novo incidente. Isso não exclui, porém, que a organização também trabalhou com períodos de opacidade que podem ter maximizado as vulnerabilidades de seus usuários. Isto porque o primeiro comunicado saiu apenas dias depois do ataque. O segundo, quatro dias após o primeiro. Ao final, os jogadores passaram quase duas semanas esperando um posicionamento definitivo sobre o que ocorreu e como poderiam agir para se proteger.

Entendemos que a organização precisou investigar o ataque antes de disponibilizar mais informações, porém a disputa de sentidos entre a reclamação de instabilidade e o silêncio da conta oficial do jogo durante esse período mostra uma tentativa de adotar mecanismos de invisibilidade para não precisar declarar o que estava acontecendo naquele momento. No comunicado, a Riot Games afirma que a invasão foi bloqueada após algumas horas. Isto é, se ele ocorreu no início da semana e após algumas horas já tinha sido neutralizado, o aviso ao público também poderia ter sido mais rápido.

Além de analisar situações como essa, a presente pesquisa propõe a abertura de futuros trabalhos que possam entender outros setores organizacionais e como eles lidam com a utilização de transparência. Além disso, vale pontuar a necessidade de mais estudos que questionem o *accountability* e o posicionamento das organizações, prevendo padrões que podem minimizar as vulnerabilidades dos públicos, permitindo maiores cobranças no futuro.

Referências

ALÓ, C. **Uma abordagem para transparência em processos organizacionais utilizando aspectos**. Tese apresentada ao Programa de Pós-Graduação em Informática da Pontifícia Universidade Católica

do Rio de Janeiro, 2009. Disponível em: https://www-di.inf.puc-rio.br/~julio/tese-cappelli.pdf. Acesso em 01 fevereiro 2024.

ARAUJO, F.; ROSSI, J. **A evolução dos ataques cibernéticos**. Trabalho de Conclusão de Curso - Segurança da Informação, Faculdade de Tecnologia de Americana, Americana/SP, 2020. Disponível em: http://ric.cps.sp.gov.br/bitstream/123456789/5272/1/1S2020_Franciele%20Cassimiro%20de%20Ara%C3%BAjo_OD0878.pdf. Acesso em 01 de junho de 2022.

BALDISSERA, R. Comunicação organizacional na perspectiva da complexidade. **Organicom**, v. 6, n. 10, 2009. Disponível em: https://www.revistas.usp.br/organicom/article/view/139013. Acesso em 19 fevereiro 2024.

BARDIN, L. **Análise de conteúdo**. São Paulo: Edições 70, 2011.

BRASIL. **Constituição Federal**. 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 19 fevereiro 2024.

BRASIL. **Lei nº 12.527** (Lei de Acesso à Informação). 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em 15 março 2021.

CAMPOS, D. **O pensamento formal no jogo digital League of Legends: As características funcionais**. Dissertação apresentada ao Programa de Pós-Graduação em Educação da Universidade Federal do Triângulo Mineiro, 2022. Disponível em: http://200.131.62.27/handle/123456789/1471. Acesso em 01 fevereiro 2024.

CUNHA FILHO, M. O que sabemos sobre transparência pública? Uma revisão bibliográfica das abordagens normativa, conceitualista e empírica. **Revista da CGU**, v.10, n. 16. 2018. Disponível em: https://ojs.cgu.gov.br/index.php/Revista_da_CGU/article/view/144. Acesso em: 20 de junho de 2022.

DIAS, C. **O conceito de transparência empresarial: reflexões a partir de uma meta-análise**. Dissertação de Mestrado em Gestão da Universidade Católica Portuguesa, Porto, 2016. Disponível em: https://repositorio.ucp.pt/bitstream/10400.14/21653/1/Disserta%C3%A7%C3%A3o_O%20conceito%20de%20transparencia%20empresarial_CarlaDias.pdf. Acesso em 19 fevereiro 2024.

GOMES, W. Participação política online: questões e hipóteses de trabalho. In: MAIA, R. *et al.* (Org.). **Internet e participação política no Brasil**. Porto Alegre: Sulina, 2017.

LIMA, G. Ciberataques: uma reflexão sobre a responsabilidade internacional dos estados. **Caderno de Relações Internacionais**, v. 8, n. 15, 2017. Disponível em: https://revistas.faculdadedamas.edu.br/index.php/relacoesinternacionais/article/view/646. Acesso em 08 novembro 2022.

LUCCHESE, F.; RIBEIRO, B. **Conceituação de Jogos Digitais**. FEEC/Universidade Estadual de Campinas Cidade Universitária Zeferino Vaz, Campinas, 2009. Disponível em: https://www.dca.fee.unicamp.br/~martino/disciplinas/ia369/trabalhos/t1g3. Acesso em 21 fevereiro 2024.

MARTINS FILHO, V. *et al.* Design thinking, cognição e educação no século XXI. **Rev. Diálogo Educ.**, Curitiba, v. 15, n. 45, p. 579-596, maio/ago. 2015.

RINCÓN, M. Análisis de la transparencia organizacional y el poder económico a partir la teoría de juegos. **Revista Universidad y Empresa**, v. 22, n. 38, 2020.

SILVA, S. Transparência digital em instituições democráticas: horizontes, limites e barreiras. In: MENDONÇA, R. *et al.* (Org). **Democracia digital: publicidade, instituições e confronto político**. Belo Horizonte: Editora UFMG, 2016.

SILVA, F. *et al.* Ética e transparência organizacional. **Revista Sociedade em Debate**, v. 4, n. 2, 2022.

SILVA, D. **Comunicação organizacional e as estratégias de invisibilidade e de redução/direcionamento da visibilidade nas mídias sociais**. Tese de Doutorado apresentada ao Programa de Pós-Graduação da Universidade Federal do Rio Grande do Sul, Porto Alegre, 2018. Disponível em: https://lume.ufrgs.br/handle/10183/180564. Acesso em 21 de maio de 2023.

VELLO, B. **Inovação democrática e desconfiança: o controle das políticas públicas nos conselhos**. Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Ciência Política da Universidade de São Paulo. São Paulo, 2017. Disponível em: https://www.teses.usp.br/teses/disponiveis/8/8131/tde-10072018-155747/publico/2017_BrunoGrisottoVello_VOrig.pdf. Acesso em 17 maio 2023.

VIEIRA, S. *et al.* A importância e a adoção das práticas de governança corporativa a luz do princípio da transparência: um estudo de caso em uma empresa do setor de não tecidos. **Perspectiva**, v. 39, n. 146, 2015. Disponível em: https://www.uricer.edu.br/site/pdfs/perspectiva/146_515.pdf. Acesso em 01 novembro 2022.

WALTERS, R. **Cyber Attacks on U.S. Companies Since November 2014**. Report Cybersecurity, The Heritage Foundation, 2015. Disponível em: https://www.heritage.org/cybersecurity/report/cyber-attacks-us-companies-november-2014. Acesso em 08 novembro 2022.

WILLIAMS, C. C. Trust Diffusion: The Effect of Interpersonal Trust on Structure, Function, and Organizational Transparency. **Business & Society**, Boston University, v. 44, n. 3, p. 1- 357, 2005.