Научная статья

УДК 343.713
DOI 10.25205/2542-0410-2025-21-2-61-67

Угроза как способ совершения преступлений против собственности: концепция «чувствительной» информации

Роман Николаевич Боровских[1]
Ольга Валерьевна Шмыгина[2]

[1]Новосибирский государственный университет
Новосибирск, Россия

[2]Сибирский университет потребительской кооперации
Новосибирск, Россия

[1]mail@rborovskih.ru
[2]olga78an1@rambler.ru

Аннотация

В статье рассматриваются актуальные проблемы юридической оценки использования различного рода информации при совершении преступлений против собственности. В результате проведенного исследования сформулировано несколько критериев, которые наделяют определенную информацию качеством «чувствительность». Делается вывод о том, что качество угрозы может приобрести любая информация, исходя из ее содержания, формы, выражения и трансляции адресату, а также особенностей субъективного восприятия адресатами такой информации.

Ключевые слова

угроза, шантаж, имущество, информация, информационная безопасность, сталкинг, уголовная ответственность

Для цитирования

Боровских Р. Н., Шмыгина О. В. Угроза как способ совершения преступлений против собственности: концепция «чувствительной» информации // Юридическая наука и практика. 2025. Т. 21, № 2. С. 61–67. DOI 10.25205/2542-0410-2025-21-2-61-67

Threat as a Way of Committing Crimes Against Property: the Concept of “Sensitive” Information

Roman N. Borovskikh[1], Olga V. Shmygina[2]

[1]Novosibirsk National Research State University
Novosibirsk, Russian Federation

[2]Siberian University of Consumer Cooperation
Novosibirsk, Russian Federation

[1]mail@rborovskih.ru
[2]olga78an1@rambler.ru

Abstract

The article discusses the current problems of legal assessment of the use of various types of information in the commission of crimes against property. As a result of the conducted research, several criteria have been formulated that endow certain information with the quality of “sensitivity”. It is concluded that any information can acquire the quality

of a threat based on its content, form, expression and transmission to the addressee, as well as the peculiarities of the addressees' subjective perception of such information.

Keywords

threat, blackmail, property, information, information security, stalking, criminal liability

For citation

Borovskikh R. N., Shmygina O. V. Threat as a way of committing crimes against property: the concept of "sensitive" information. *Juridical Science and Practice*, 2025, vol. 21, no. 2, pp. 61–67. (in Russ.) DOI 10.25205/2542-0410-2025-21-2-61-67

В современном обществе, в условиях повсеместной информатизации, компьютеризации, роботизации, виртуализации, цифровизации и т. п., многие сущности, в том числе правовые, должны рассматриваться через «призму» информации, концепт информации. Является закономерным, что концепт «информация» широко представлен исследованиях, посвященных вопросам правового регулирования и правовой охраны общественных отношений, и уголовно-правовые исследования также не являются исключением.

Разумеется, информация – еще не есть угроза. Далеко не любая информация, доведенная до сведения человека, становится для него угрожающей. Здесь даже возможны любопытные противоположности: так, негативная информация о человеке, т. е. объективно содержащая для него угрозу, нередко не воспринимается им в таком качестве (например, когда адресат не имеет оснований опасаться такой угрозы); и, наоборот, часто вполне нейтральные либо, в ряде случаев, положительные сведения могут быть для их адресата серьезной угрозой (например, информация о человеке как владельце крупного денежного приза и т. д.). В современной правоприменительной практике можно обнаружить немало примеров вымогательских требований и других преступных действий, совершаемых под угрозой придания гласности информации о каких-либо конфиденциальных обстоятельствах личной и общественной жизни человека. Свежи в памяти примеры вымогательства в отношении высокопоставленных лиц и медийных персон, совершенные администраторами телеграм-каналов и владельцев пабликов в социальных сетях [1].

Информационный портал лаборатории Касперского называет подобные деяния доксингом – от англ. сленговых слов «drop dox» (скинуть документы), «dox» (документы). Речь идет о ситуациях, когда требование передачи имущества сопровождается угрозой собирать из открытых источников и распространять (делать «вбросы» в информационное пространство) разнообразной информации о человеке, не относящейся к личной или иной тайне (его хобби, увлечениях, приобретениях, посещении им публичных мест, знакомствах, награждении, работе и пр.). Важно отметить, что уголовно-правовая оценка содеянного как вымогательства в таких случаях не всегда является возможной. Причиной тому является формальное несоответствие той информации, которую злоумышленники обещают придать огласке, пониманию угрозы в традиционном уголовно-правовом смысле [2, с. 144]. В уголовно-правовой литературе подобное преследование со стороны недобросовестных журналистов и других лиц иногда называют сталкингом или сталкерством [3, с. 29–35].

В Интернете можно найти много примеров рассматриваемых общественно опасных практик, когда в целях совершения преступлений против собственности злоумышленниками используется определенная (часто внешне безобидная) информация: использование шерентинга (размещения родителями чрезмерного контента о детях в социальных сетях), груминга (тесной дружба для дальнейшей эксплуатации), «темных» паттернов (вводящих в заблуждение дизайнов интерфейсов) и другой дезинформации. Специалисты предупреждают, что серьезным имущественным ущербом угрожает обернуться обладание и использование хакерами такой незначительной информации, как адрес личной электронной почты.

Весьма любопытны в рассматриваемом плане исследования, которые показывают, что пригодную для целей шантажа информацию злоумышленники могут получить на основании контент-анализа любой информации, «потребляемой» человеком в информационном пространстве, поскольку такая информация есть форма проявления идентичности человека, т. е. информация о нем самом [4, с. 98–119].

Из приведенных примеров и рассуждений следует вывод о том, что качество угрозы может приобрести любая информация, исходя из определенных факторов: конкретного содержания, формы и нюансов выражения и трансляции адресату, а также особенностей субъективного восприятия адресатами такой информации. Возникает вопрос: возможно ли существование некой интегративной характеристики всех подобных факторов, которая определяла бы конвертацию определенной информации в угрозу и являлась бы пригодной для целей уголовно-правовой характеристики соответствующих имущественных и иных преступлений.

Существующее в научной литературе понимание того, когда определенная информация может становиться уголовно-релевантной угрозой, в основном связано с критериями оценки реальности такой угрозы. Имеющиеся подходы к определению реальности угрозы можно классифицировать как субъективный, объективный, субъективно-объективный. Данная классификация зависит от того, какой смысл вкладывают сторонники того или иного подхода в оценку реальности угрозы.

Возможно выделить следующий классический перечень критериев реальности угрозы:

1) основания опасаться ее исполнения: эти основания обусловлены субъективной оценкой обстоятельств получения угрозы, а также иных сведений, имеющихся в распоряжении потерпевшего, лица, к которому эта угроза была обращена;

2) форма угрозы: оценка потерпевшим угрозы как реальной может быть связана со способом получения требования вымогателя, но этот способ не влияет на квалификацию действий как вымогательства, хотя форма угрозы, например, конклюдентные действия, может свидетельствовать о намерении вымогателя привести ее в исполнение (например, виновный подошел к потерпевшим с ружьем, произвел выстрел в землю, потребовал передачи ему денежных средств; угрозы он не высказывал, но потерпевшие имели основания опасаться наступления отрицательных последствий, обусловленных последующими действиями со стороны виновного)[1];

3) угроза необязательно может быть реализована незамедлительно, это могут быть действия, совершаемые виновным в последующем, если потерпевший не выполнит его требования.

Показательна ситуация массовой, многоадресной рассылки электронных писем о якобы имевшем место аморальном поведении адресата, с требованием передачи денежных средств за неразглашение таких сведений. Злоумышленник действует в таком случае наугад. Получатель информации уверен, что угроза в такой информации реально не осуществима (например, аморального поведения с его стороны не было), но и транслятор информации-угрозы не имеет достаточных оснований считать, что его угроза возымеет действие. При всем этом рассылаемая информация, очевидно, получает «эффект», качество угрозы. Критерий реальности угрозы в таких случаях оказывается не вполне пригодным. Следовательно, повторим, качество угрозы информация приобретает далеко не только исходя из критерия реальности соответствующей угрозы. В этой связи полагаем и предлагаем, что искомой интегративной характеристикой может выступать категория «чувствительности» информации или концепт «чувствительной» информации.

[1] Приговор Коченевского районного суда Новосибирской области от 25.09.2019 по делу № 1-147/2019 // Судебные решения РФ. URL: https://судебныерешения.рф/44473737 (дата обращения: 20.02.2025).

Словосочетание «чувствительная информация», при всем очевидном скепсисе в ее юридическом измерении, в последнее время стало весьма популярным в информационном пространстве [5] и научной литературе [6, с. 42–46].

Как правило, термин «чувствительная информация» используется в сфере финансов: это информация, несанкционированное раскрытие, модификация или сокрытие которой может привести к ощутимому убытку или (денежному) ущербу.

В российском нормативном поле данный термин в настоящее время отсутствует, однако следует упомянуть об отдельных попытках законодателей предложить законопроекты, где данный термин использовался.

Так, например, по информации главы комиссии Совета Федерации РФ по защите государственного суверенитета А. Климова, в 2020 г. парламентариями был разработан законопроект об изменениях в УК РФ, который предусматривал «…норму о наказании для физлиц, занимающихся сбором информации чувствительного характера и нарушающего законодательство об иноагентах» [7]. В результате в соответствующем законопроекте была исключена формулировка «чувствительные данные», а сам законопроект снят с рассмотрения[2].

Однако в правоприменительной практике можно встретить судебные решения, где термин «чувствительная информация» упоминается[3].

Полагаем верным исходить из того, что «чувствительная» информация – это, прежде всего, информация ограниченного доступа.

С учетом сказанного сформулируем далее несколько критериев, которые, на наш взгляд, наделяют определенную информацию качеством «чувствительность».

Во-первых, характер информации (здесь укажем, что такой характер может быть негативным, социально нейтральным и, в ряде случаев, социально положительным). Это могут быть клеветнические заявления и диффамационные сведения о порочащих поступках, а также иная компрометирующая человека информация. Также следует обратить внимание на проблему оценки высказанных суждений как личного мнения или утверждения о факте. В современной практике негативная информация часто предается огласке с оговоркой о личном мнении, что в ряде случаев нейтрализует возможности ее юридической оценки как компрометирующей и, как следствие, уголовно-релевантной [8, с. 129–133].

Не менее проблематичными являются ситуации, когда характер информации при угрозе предстает в социально нейтральном либо даже социально положительном свете. Здесь показателен пример, связанный с информаций о поведении человека в сфере электронной коммерции.

Так, специалисты утверждают, что любой человек, как потенциальный или реальный покупатель товаров и услуг в Интернете, оставляет определенную информацию – так называемый «экономический след», которую возможно использовать как угрозу.

Видно, что большинство из указанных сведений носят, как правило, социально нейтральный характер, но вполне могут быть использованы злоумышленником в качестве «чувствительной» информации и конвертированы в угрозу при совершении вымогательства или другого преступления против собственности. То же самое можно сказать о случаях, когда в преступных целях как угроза может быть использована социально-положительная информация (например, о человеке как об участнике специальной военной операции либо как о победителе лотереи, получателе крупного денежного приза и т. п.).

---

[2] Законопроект № 1057914-7 «О внесении изменений в отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия угрозам национальной безопасности» // Портал «Система обеспечения законодательной деятельности». URL: https://sozd.duma.gov.ru/bill/1057914-7 (дата обращения: 22.02.2025).

[3] Определение № А40-132453/2021 от 18.05.2022 Арбитражного Суда Московского округа // Чувствительная информация – гражданское законодательство и судебные прецеденты. URL: https://lawnotes.ru/podborki-gk-rf/chuvstvitelnaya-informatsiya (дата обращения: 22.02.2025).

Таким образом, характер информации – важный, но не единственный критерий отнесения информации к категории «чувствительная».

Во-вторых, контекст передачи (объективации, выражения, трансляции) информации, учитывающий форму и обстановку выражения, а также сопутствующую транслируемым сведениям дополнительную информацию (фон). Например, весьма распространенным явлением является так называемый «шерентинг» (от англ. sharenting – сочетание англ. слов share – совместное использование и parenting – воспитание), представляющий собой практику родителей публиковать большое количество потенциально конфиденциального контента о своих детях на интернет-платформах. Как верно указывают специалисты, «шерентинг таит в себе и много опасностей, таких как кража персональных данных и потенциальное внимание со стороны злоумышленников. Кроме того, шерентинг может привести к негативным последствиям для ребенка, когда он вырастет. Например, повлиять на возможности его трудоустройства»[4]. В частности, такая информация может быть конвертирована преступником в угрозу путем направления потерпевшему фотографий и видеозаписей о его детях и близких, без какого-либо текста, но с «намеком» на слежку за ребенком, его преследование, контроль за ним, сексуальный интерес и т. п.

В-третьих, особенности субъективного восприятия конкретным адресатом информации. Здесь важную роль играют мотивы, эмоции, установки и социальный опыт человека; когнитивные процессы (когда человек осмысливает информацию, руководствуясь необходимостью сформировать понятную ему картину реальности, подчиняя осмысление фактов эмоциям и потребностям); социально-культурные особенности человека, его половозрастные характеристики и т. д.

Специалисты отмечают, что информационная безопасность является серьезной психологической проблемой, поскольку «особенности информационного воздействия состоят в том, что, кроме специальных технологий воздействия, используются приемы, направленные на запугивание людей и, что самое главное, на нивелирование их собственной активности, направленной на проверку поступающей информации и ее селекцию» [9, с. 45–46].

Сказанное убеждает в том, что субъективно воспринимаемая информация часто является для конкретного человека чувствительной и, как следствие, может использоваться для формирования угрозы в отношении этого человека.

С учетом изложенного представляется возможным определить понятие «чувствительная информация» следующим образом: это информация негативного, социально нейтрального либо, в ряде случаев, социально положительного характера, которая в зависимости от контекста ее передачи адресату и его субъективного восприятия данной информации при распространении (огласке) представляет угрозу правам и законным интересам адресата, его близких либо иных лиц, а также способна причинить указанным лицам моральный вред и (или) имущественный ущерб.

Список литературы

1. **Александров А.** Блок не помешал процессу. Администраторов Telegram-каналов судят за вымогательства // Коммерсантъ. 2024. 3 янв. URL: https://www.kommersant.ru/doc/6428797 (дата обращения: 27.02.2025).
2. **Овсюков Д. А.** Использование информационно-телекоммуникационных сетей при совершении вымогательства // Актуальные проблемы российского права. 2022. Т. 16, № 2. С. 144.

[4] О чем должны подумать родители, прежде чем публиковать фотографии детей в Интернете // Информационный портал «Kaspersky». URL: https://www.kaspersky.ru/resource-center/threats/children-photos-and-online-safety (дата обращения: 27.02.2025).

3. **Куликов А. В., Егорычева Е. А.** Проблемы и перспективы криминализации сталкинга в России // Известия ТулГУ. Экономические и юридические науки. 2022. № 3. С. 29–35.
4. **Шилова В. А., Яковлева А. А.** Потребление информации как форма проявления идентичности (ч. 1) // Коммуникации. Медиа. Дизайн. 2021. Т. 6, № 2. С. 98–119.
5. Чувствительные данные: как отделить важное от обычного. Информационный портал «Securitymedia.org». URL: https://securitymedia.org/info/chuvstvitelnye-dannye-kak-otdelit-vazhnoe-ot-obychnogo.html (дата обращения: 27.02.2025).
6. **Сидак А. А.** Вопросы применения на объектах критической информационной инфраструктуры инновационных автоматизированных рабочих мест Интернет, обеспечивающих защиту чувствительной речевой и визуальной информации // Информационные войны. 2023. № 4 (68). С. 42–46.
7. В Совфеде предложили сажать иноагентов за сбор чувствительной информации // Информационный портал «RBK». URL: https://www.rbc.ru/society/27/11/2020/5fc14a0d9a79476ebc96b739 (дата обращения: 22.02.2025).
8. **Гаджиалиева Н. Ш., Абдурахманов Д. К.** Разграничение утверждений о фактах и оценочных суждений при разрешении диффамационных споров // Вестник Дагестан. гос. ун-та. Серия 3: Общественные науки. 2018. № 3. С. 129–133.
9. **Тарабрина Н. В., Харламенкова Н. Е., Падун М. А., Хажуев И. С., Казымова Н. Н., Быховец Ю. В., Дан М. В.** Интенсивный стресс в контексте психологической безопасности; под общ. ред. Н. Е. Харламенковой. М.: Институт психологии РАН, 2017. С. 45–46.

References

1. **Alexandrov A.** Blok did not interfere with the process. Administrators of Telegram channels are being tried for extortion. *Kommersant newspaper*. 2024. 3 Jan. URL: https://www.kommersant.ru/doc/6428797 (date of request: 02/27/2025).
2. **Ovsyukov D. A.** The use of information and telecommunication networks in the commission of extortion. *Actual problems of Russian law*, 2022, vol. 16, no. 2, pp. 144. (in Russ.)
3. **Kulikov A. V., Egorycheva E. A.** Problems and prospects of criminalization of stalking in Russia. *Izvestiya TulSU. Economic and legal sciences*, 2022, no. 3, pp. 29–35. (in Russ.)
4. **Shilova V. A., Yakovleva A. A.** Information consumption as a form of identity manifestation (part 1). *Communications. Media. Design*, 2021, vol. 6, no. 2, pp. 98–119. (in Russ.)
5. Sensitive data: how to separate the important from the ordinary. Information portal “Securitymedia.org”. URL: https://securitymedia.org/info/chuvstvitelnye-dannye-kak-otdelit-vazhnoe-ot-obychnogo.html (date of request: 02/27/2025). (in Russ.)
6. **Sidak A. A.** Issues of the use of innovative automated Internet workstations at critical information infrastructure facilities that protect sensitive speech and visual information. *Information Wars*, 2023, № 4(68), pp. 42–46. (in Russ.)
7. The Federation Council proposed to imprison foreign agents for collecting sensitive information. *RBK Information Portal*. URL: https://www.rbc.ru/society/27/11/2020/5fc14a0d9a79476ebc96b739 (date of request: 02/22/2025).
8. **Gadzhialieva N. S., Abdurakhmanov D. K.** Differentiation of statements about facts and value judgments in resolving defamation disputes. *Bulletin of Dagestan State University*. Series 3: Social Sciences, 2018, no. 3, pp. 129–133. (in Russ.)
9. **Tarabrina N. V., Kharlamenkova N. E., Padun M. A., Khazhuev I. S., Kazymova N. N., Bykhovets Yu. V., Dan M. V.** Intense stress in the context of psychological safety; ed. by N. E. Kharlamenkova. Moscow, Publishing House “Institute of Psychology of the Russian Academy of Sciences”, 2017, pp. 45–46. (in Russ.)

Информация об авторах

Боровских Роман Николаевич, профессор кафедры уголовного права, уголовного процесса и криминалистики Новосибирского государственного университета

Шмыгина Ольга Валерьевна, старший преподаватель Сибирского университета потребительской кооперации

Information about the Authors

Roman N. Borovskikh, Professor of the Department of Criminal Law, Criminal Procedure and Criminalistics of Novosibirsk National Research State University Novosibirsk, Russian Federation

Olga V. Shmygina, Senior Lecturer, Siberian University of Consumer Cooperation (SibUPK) (Novosibirsk, Russian Federation)

Статья поступила в редакцию 18.03.2025;
одобрена после рецензирования 20.03.2025; принята к публикации 21.03.2025

The article was submitted 18.03.2025;
approved after reviewing 20.03.2025; accepted for publication 21.03.2025